Miscellaneous

9. The State Nodal Department should not share the SRDH code and assets with agencies, other than their own System Integrator (SI's) and agencies working for them on Aadhaar working for them on Aadhaar enabled service projects and initiatives, with a condition that the SI's or Agencies would not redistribute further or make copies.

10. The State Nodal Department needs to adhere to UIDAI's data security policies to keep Aadhaar enrolment data source.

11. Any provision of this MoU may be amended or waived if, and only if, such amendment or waiver is evidenced by a written instrument signed by duly authorised representatives of the Parties, or, in the case of waiver, by the Party against whom the waiver is to be effective.

IN WITNESS WHEREOF, the undersigned have executed this MoU, in duplicate, as of the date set forth above.

14/1/2013

(For UIDAI)
Amit Singal
Asst. Director General, UIDAI
Govt. of India, R.O., Chandigarh

(For State Nodal Department)

(TRUE COPY)

Joint Secretary
Deptt. of Food, Civil Supplies
& Consumer Affairs, Pb.,
Chandigarh.

IN THE SUPREME COURT OF INDIA

APPELLATE JURISDICTION (CIVIL)

WRIT PETITION (CIVIL) NO.932 OF 2013

IN THE MATTER OF :

NAGRIK CHETNA MANCH. .... PETITIONER

Versus

UNION OF INDIA & ORS. .. RESPONDENTS

PAPER BOOK

(Counter Affidavit of R-4)

(FOR INDEX, PLEASE SEE INSIDE)

(ADVOCATE FOR THE RESPONDENT NO.4. **H.S. PARIHAR**)

INDEX

IN THE SUPREME COURT OF INDIA

APPELLATE JURISDICTION (CIVIL)

WRIT PETITION (CIVIL) NO.932 OF 2013

IN THE MATTER OF :

NAGRIK CHETNA MANCH. .... PETITIONER

Versus

UNION OF INDIA & ORS. .. RESPONDENTS

COUNTER AFFIDAVIT ON BEHALF OF RESPONDENT NO.4 RESERVE BANK OF INDIA

I, Rahul Sinha, son of Shri Bhola Nath Sinha, aged about 42 years, residing at M-5 RBI Officers Flats, Vasant Vihar, New Delhi-110057, do hereby solemnly affirm and say as follows:

I. That I am working as Deputy General Manager in the Reserve Bank of India, Department of Banking Supervision, Regional Office, New Delhi. I am competent and authorized to affirm this affidavit on behalf of the Reserve Bank of India (hereinafter referred to as "RBI"/Reserve Bank/this Respondent or answering Respondent). I have gone through the averments made in the said Writ Petition. I am well conversant with the facts of the case and issues in the captioned Writ Petition. I have access to all the records pertaining to the case kept with Respondent No.4 and after going through the same and having made myself fully acquainted with the facts of this case, I am filing this affidavit.

II. PRELIMINARY OBJECTIONS

(i) At the outset, it is submitted that there is no violation of any fundamental, statutory or legal right of the Petitioner by Respondent No.4 and as such the present Writ Petition, under Article 32 of the Constitution of India is wholly misconceived and not maintainable, either in law or on facts, against this Respondent, and the Writ Petition is liable to be dismissed with costs.

(ii)This affidavit is being filed by RBI for the limited purpose of apprising this Hon'ble Court of the position regarding the instructions issued by Reserve Bank, which are in some way related to the issues referred to in the writ petition. I reserve liberty to file a further Affidavit, if found necessary, at a later stage.

SUBMISSION ON THE POSITION OF RBI

(i) The Respondent No.4, Reserve Bank of India is a statutory Corporation constituted by the provisions of Section 3 of the Reserve Bank of India Act, 1934 for the purpose of regulating the issue of Bank Notes and keeping of reserves with a view to secure the monetary stability in India and generally to operate currency and credit system of the country. The Reserve Bank has been, *inter alia*, entrusted with the statutory obligation of administering the provisions of the Banking Regulation Act, 1949 (the "**BR Act**"). Under the BR Act, RBI has been vested with various powers with respect to banking companies, such as granting licenses, conducting inspections, giving directions, advices etc.

(ii) As the principal monetary authority in the country, RBI is responsible for laying down policies in the interest of the monetary

stability and sound economic growth, having due regard to the interests of the depositors, public interest and banking policy. In the discharge of its statutory duties, RBI issues various guidelines and directions to the banks. RBI has the power to issue directions under Section 35A of the BR Act to banks generally or any bank in particular in the public interest or in the interest of the banking policy or to prevent the affairs of the bank from being conducted in a manner detrimental to the interests of the depositors or in a manner prejudicial to the bank or to secure the proper management of any bank. RBI also has the power under Section 36(1) (a) of the BR Act, to caution or prohibit banks generally or any bank in particular against entering into any transaction or class of transactions and to generally give advice to any bank. RBI being an expert body, its decisions with regard to the regulation of banks, deserve to be given due weightage.

Background

1. It is submitted that Government of India (GoI) has launched the Direct Benefit Transfer (DBT) Scheme. Reserve Bank's instructions to banks relate to opening of accounts for facilitating the DBT and they have not instructed banks to launch or introduce DBT. In addition to the above, Reserve Bank of India has formulated the Know Your Customer (KYC) norms/Anti-Money Laundering (AML) standards/Combating of Financing of Terrorism (CFT) guidelines to be followed by banks, so as to prevent banks from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities. KYC procedures also enable banks to know/understand their customers and their financial dealings better, which in turn help them manage their risks prudently. Accordingly, Reserve Bank has issued instructions to all

banks under the relevant provisions of the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, to follow certain customer identification procedures for opening of accounts and monitoring transactions of a suspicious nature for the purpose of reporting it to appropriate authority, i.e. Financial Intelligence Unit-India. Banks have also been advised to ensure that a proper policy framework on KYC/AML/CFT is formulated with the approval of their Board and put in place.

2. It is submitted that in terms of the guidelines issued by Reserve Bank of India which are consolidated in the Master Circular dated July 1, 2014 on KYC norms/ AML standards/ CFT, banks while framing their KYC policies should incorporate the four key elements viz; Customer Acceptance Policy, Customer Identification Procedures, Monitoring of Transactions and Risk Management. The details of Customer Acceptance Policy and Identification Procedures are as follows:

a) Banks have been advised to have a Customer Acceptance Policy which ensures that no account is opened in anonymous or fictitious/benami name, clearly defines parameters of risk perception, documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of Prevention of Money Laundering Act, 2002 (hereinafter referred to as 'PMLA'), not to open an account where the bank is unable to apply appropriate customer due diligence measures and apply necessary checks before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organisations etc. Banks have also been

advised to consider closing an existing account under similar circumstances and to have suitable built -in safeguards to avoid harassment of a customer.

b) Banks have been advised to frame a policy approved by their Boards and they should clearly spell out the Customer Identification Procedure to be carried out at different stages, i.e., while establishing a banking relationship; carrying out a financial transaction or when the bank has a doubt about the authenticity/veracity or adequacy of the previously obtained customer identification data. Customer identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information. Banks need to obtain sufficient information necessary to establish, to their satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of banking relationship.

3. It is submitted that an indicative list of documents required to open a bank account is given in Annex I of the RBI Master circular dated July 1, 2014 based on the PMLA and Rules framed thereunder. A copy of the Master circular is annexed hereto and marked as **ANNEXURE R-IV/1**. It is submitted that 'Aadhaar' (the letter issued by the Unique Identification Authority of India (UIDAI) containing details of name, address and Aadhaar number) is one of the documents included in this list.

4. It is submitted that for opening a bank account, Rule 9 of the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (hereinafter referred to as '**PML Rules**') requires a client who is an individual to submit, *interalia*, a certified copy of an "*officially*

valid document" (OVD) containing details of his identity and address. The expression "officially valid document" as defined in Rule 2(d) of PML Rules means various documents like passport, driving licence etc. mentioned therein and it includes ' the letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number". It is therefore submitted that Aadhar is not the sole KYC document insisted upon for opening a bank account. It is only one of the documents that can be used by the customer as an officially valid document for the purpose of opening a bank account.

5. It is further submitted that as a part of risk monitoring, it has been advised in paragraph 2.13 of the Master Circular that ongoing monitoring is an essential element of effective KYC procedures. Banks can effectively control and reduce their risk only if they have an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. Banks have been advised to pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. Banks have been advised that transactions that involve large amounts of cash, inconsistent with the normal and expected activity of the customer should particularly attract the attention of banks and very high account turnover, inconsistent with the size of the balance maintained may indicate that funds are being 'washed' through the account. High-risk accounts have to be subjected to intensive monitoring. Banks have been advised to set key indicators for such accounts, taking note of the background of the customer, such as the country of origin, sources of funds, the type of transactions involved and other risk factors. Banks have been advised to put in place a system of

periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures. Such review of risk categorisation of customers should be carried out at a periodicity of **not less** than once in six months.

6. It is submitted that these instructions enable banks to identify their customers and monitor their transactions to identify and report any suspicious transactions which in turn help them manage their risks prudently. Further, paragraph 2.25 (b) of the Master Circular dated July 1, 2014 ,lays down the instructions for banks for determining and reporting of suspicious transaction reports. The details are as follows:

A. Suspicious Transaction Reports (STRs)

i) While determining suspicious transactions, banks should be guided by the definition of suspicious transaction contained in PMLA Rules, as amended from time to time.

ii) It is likely that in some cases transactions are abandoned /aborted by customers on being asked to give some details or to provide documents. The banks should report all such attempted transactions in STRs, even if not completed by customers, irrespective of the amount of the transaction.

iii) Banks should make STR if they have a reasonable ground to believe that the transaction involves proceeds of crime generally, irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences in part B of Schedule of PMLA, 2002.

iv) The Suspicious Transaction Report (STR) should be furnished within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of a suspicious nature. The Principal Officer should record his reasons for treating any transaction or a series of transactions as suspicious. Banks should ensure that there is no undue delay in arriving at such a conclusion once a suspicious transaction report is received from a branch or any other office. Such report should be made available to the competent authorities on request.

v) In the context of creating KYC/AML awareness among the staff and for generating alerts for suspicious transactions, banks have been advised to consider the indicative list of suspicious activities contained in Annex-E of the 'IBA's Guidance Note for Banks, January 2012'.

vi) Banks should not put any restrictions on operations in the accounts where an STR has been made. Banks and their employees should keep the fact of furnishing of STR strictly confidential, as required under PML Rules. It should be ensured that there is no tipping off to the customer at any level.

B. Cash Transaction Reports (CTRs)

CTRs must be filed by the banks in respect of following transactions:

* all cash transactions of value more than Rupees Ten Lakh or its equivalent in foreign currency;

* all series of cash transactions integrally connected to each other which have been valued below Rupees Ten Lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds Rupees Ten Lakh;

1. It is submitted that banks are required to report information related to STRs/ CTRs to the Director, Financial Intelligence Unit-India (FIU-IND). These obligations are required to be complied with by the banks, irrespective of whether the account is opened with Aadhar as the officially valid document or not and this mechanism is intended to detect fraudulent transactions and enable banks to manage their risks prudently.

2. It is further submitted that RBI has issued a circular bearing DBOD.AML.BC. No.29 /14.01.001/2013-14 dated July 12, 2013 whereby banks were instructed to verify the PAN numbers given by the account based as well as walk-in customers

3. In addition to the above, it is submitted that RBI has issued circular bearing DBOD AML BC No.44/14.01.001/2013-14 dated September 2, 2013 advising banks that e-KYC service of the UIDAI would be accepted as an officially valid document'. It is mentioned in the circular that while using e-KYC service of UIDAI, the individual user has to authorize the UIDAI, by explicit consent, to release her or his identity/address through biometric authentication to the bank branches/business correspondents (BCs). A copy of the circular dated September 02, 2013 is annexed hereto and marked as **ANNEXURE R-IV/2.**

4. It is submitted that the UIDAI then transfers the data of the individual comprising name, age, gender, and photograph of the individual, electronically to the bank/BCs, which may be accepted as valid process for KYC verification. The broad operational instructions to banks on Aadhaar e-KYC service are enclosed in the Annex of the circular DBOD.AML.BC. No. 44 /14.01.001/2013-14 dated September 2, 2013 and the procedure makes it mandatory for the bank to enter into an agreement with the UIDAI. Banks are required to fulfill certain conditions such as defining a procedure for obtaining customer authorization to UIDAI for sharing e-KYC data with the bank. This authorization can be in **physical** (by way of a written explicit consent authorizing UIDAI to share his/her Aadhaar data with the bank/BC for the purpose of opening bank account) / **electronic** form as defined by UIDAI from time to time.

5. It is submitted that the sample process flow would be as follows:

a. Customer walks into Customer Service point (CSP) of a bank with **his/her 12 digit Aadhaar number and explicit consent** and requests to open a bank account with Aadhaar based e-KYC.

b. Bank representative manning the CSP enters the number into bank's e-KYC application software.

c. The customer inputs his/her biometrics via a UIDAI compliant biometric reader (e.g. fingerprints on a biometric reader).

d. The software application captures the Aadhaar number along with biometric data, encrypts this data and sends it to UIDAI's Central Identities Data Repository (CIDR).

e. The Aadhaar KYC service authenticates customer data. If the Aadhaar number does not match with the biometrics, UIDAI

server responds with an error with various reasons codes depending on type of error (as defined by UIDAI).

f. If the Aadhaar number matches with the biometrics, UIDAI responds with digitally signed and encrypted demographic information [Name, year/date of birth, Gender, Address, Phone and email (if available)] and photograph. This information is captured by bank's e-KYC application and processed as needed.

g. Bank's servers auto populate the demographic data and photograph in relevant fields. It also records the full audit trail of e-KYC *viz.* source of information, digital signatures, reference number, original request generation number, machine ID for device used to generate the request, date and time stamp with full trail of message routing, UIDAI encryption date and time stamp, bank's decryption date and time stamp, etc.

h. The photograph and demographics of the customer can be seen on the screen of computer at bank branches or on a hand held device of BCs for reference.

i. The customer can open bank account subject to satisfying other account opening requirements.

5. It is submitted that the apprehension of the petitioner that a bank account can be opened solely on the basis of Aadhar is wholly misconceived. It is submitted that Aadhar is only one of the documents required for opening a bank account and not the sole KYC document for the purpose.

6. It is submitted that the Reserve Bank has issued instructions, vide its circular DBOD.AML.BC.No.65/14.01.001/2012-13 dated December 10, 2012, clarifying that if the address provided by the

account holder in the account opening form is the same as that on Aadhaar letter, then it may be accepted as both proof of identity and address since as per the earlier instruction Aadhaar letter was accepted only as a proof of identity. These instructions are applicable to all other officially valid documents used as identity proof such as Passport, Drivers' License, Voter's Identity card etc., as mentioned in para 2.(i) of the above circular.

7. As regards the apprehension expressed by the petitioner whether it is possible to open an account in the bank without being physically present, it is submitted that when the accounts are opened with e-KYC process based on Aadhaar card, the prospective customer has to remain present for biometric authentication. In other cases, accounts can also be opened without the customer being physically present. Such type of customers are treated as non-face-to-face customers. Instructions in this regard have been issued by Reserve Bank and the same are contained in paragraph 2.5(g) of the Master Circular dated July 1, 2014, which is reproduced below:

> "With the introduction of telephone and electronic banking, increasingly accounts are being opened by banks for customers without the need for the customer to visit the bank branch. In the case of non-face-to-face customers, apart from applying the usual customer identification procedures, there must be specific and adequate procedures to mitigate the higher risk involved. Certification of all the documents presented should be insisted upon and, if necessary, additional documents may be called for. In such cases, banks may also require the first payment to be effected through the customer's account with another bank which, in turn, adheres

to similar KYC standards. In the case of cross-border customers, there is the additional difficulty of matching the customer with the documentation and the bank may have to rely on third party certification/introduction. In such cases, it must be ensured that the third party is a regulated and supervised entity and has adequate KYC systems in place".

III. PARAWISE REPLY

Without prejudice to the aforesaid submissions made herein, but relying on the same, I crave leave of this Hon`ble Court to submit the parawise reply to the various averments made in the Writ Petition. All the averments made in the writ Petition, except those, which are specifically admitted, are denied. Parawise reply to the Writ Petition is submitted as under:

1. With respect to the statement of facts contained in Paragraph 1, it is submitted that the answering Respondent has no comments to offer.

2. With reference to paragraphs IA and 2 of the Writ Petition, it is submitted that the petitioner is put to strict proof.

3. With respect to the statement of facts contained in Paragraph 3, the answering Respondent has no comments to offer.

4. With respect to the averments made in paragraph 4 and 5, the petitioner is put to strict proof.

5. With respect to the averments in paragraph 6 -11 of the Writ Petition, the answering Respondent has no comments to offer as they do not relate this Respondent.

6. With reference to the averments made in paragraph 12 of the petition it is submitted that the exhibit at page 96 refers to branches of scheduled commercial banks and not rural banks. It is submitted that the concept of Business correspondents model and e-KYC process introduced by Reserve Bank eases the process of opening a bank account thus obviating the need for brick and mortar branches in every village.

7. With reference to the averments made in paragraph 13-14 of the Writ Petition, the answering Respondent has no comments to offer as it does not relate to this Respondent.

8. With reference to the averments made in paragraph 15 of the petition, the same are not fully correct. Reserve Bank has not issued any instruction stating that Aadhaar is the sole KYC document for opening "small accounts". It is submitted that Aadhaar is one of the 'Officially Valid Documents', which could be used as proof of identity and proof of address for opening a bank account. As regards opening of 'Small Accounts', it is submitted that the same is based on signature/thumb impression and photo which is certified by the designated officer that the person opening the account has affixed his signature/thumb impression in his presence, and opening of such account does not require submission of any officially valid document including aadhaar card or letter.

9. With reference to averments made in paragraphs 16 and 17 of the petition, the same are admitted to the extent revealed by records.

10. With reference to the averments made in paragraphs 18-21 of the Writ Petition, Respondent No. 4 has no comments to offer as they do not relate to this Respondent.

11. With reference to the averments made in paragraph 22 of the petition, the allegations made against this answering Respondent are denied. The Circular issued by this answering Respondent, referred to in paragraph 22, is issued to NBFCs with a view to intimate them about Govt. notification declaring Aadhaar letter as an 'officially valid document'. It is submitted that the responsibility of verifying KYC details always vests in the entity which opens accounts, and it is not correct to say that RBI has dramatically shedded its responsibility.

12. With reference to the averments made in paragraphs 23-25 of the Writ Petition, Respondent No. 4 has no comments to offer as they do not relate to this Respondent.

13. With reference to averments made in paragraph 26 of the petition, the same are admitted to the extent revealed by records. However, it is submitted that the Circular referred to in the said paragraph is regarding use of services of business correspondents.

14. With reference to averments made in paragraph 27 of the petition, the same are admitted to extent revealed by the records.

15. With reference to the averments made in paragraphs 28-31 of the Writ Petition, Respondent No. 4 has no comments to offer as they do not relate to this Respondent.

16. With reference to the averments made in paragraph 32 of the writ petition, the same are not correct. It is submitted that in terms of the extant instructions issued by the Reserve Bank, banks have to verify the identity and address of a customer when he/she approaches the bank for opening an account. It is further submitted that as per circular bearing DBOD.AML.BC. No. 44 /14.01.001/2013-14 dated September 2, 2013 issued by Reserve Bank, e-KYC service of UIDAI was accepted as a valid process for KYC verification under Prevention of Money Laundering (Maintenance of Records) Rules, 2005. It is specified in Para 2 of the circular that while using e-KYC service of UIDAI, the individual **user has to authorize the UIDAI, by explicit consent**, to release her or his identity/address **through biometric authentication** to the bank branches/business correspondents (BCs). As regards opening of 'Small Accounts', it is submitted that the same is based on signature/thumb impression and photo which is certified by the designated officer that the person opening the account has affixed his signature/thumb impression in his presence, and opening of such account does not require submission of any officially valid document including aadhaar card or letter.

17. With reference to the averments made in paragraph 33 & 34, the answering Respondent has no comments to offer as they do not relate to this Respondent.

18. With reference to the averments made in paragraph 35 of the petition, the allegations therein are not correct and hence denied. The answering Respondent reiterates the submission made herein above in preceding paragraph in response to para 32 of the counter affidavit.

19. With reference to the averments in paragraph 36 of the petition, the same are admitted to the extent revealed by the records.

20. With reference to the averments made in paragraph 37, the allegations against this Respondent are not correct and hence strongly denied., It is submitted that the petitioner has only made a vague allegation that frauds are suspected to take place in accounts opened with Aadhaar, but has not substantiated it. It is submitted that the KYC/AML/CFT guidelines are issued with the objective to prevent banks form being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities. KYC procedures also enable banks to know / understand their customers and their financial dealings better which in turn help them manage their risks prudently.

21. With reference to the averments made in paragraphs 38-41 of the Writ Petition, the answering Respondent has no comments to offer as they do not relate to this Respondent.

22. With reference to the facts stated in paragraph 42 of the petition, the same are admitted to the extent revealed by the records.

23. With reference to the averments made in paragraph 43 to 44of the petition, the answering Respondent has no comments to offer.

With reference to paragraph 45, it is submitted that the averments : "*it is thus evident that Aadhaar has unleashed a free-for-all irresponsible and highly dangerous set of procedures to open, maintain and operate bank accounts*" and that it was "*obvious that*

that the Aadhaar data and the linked bank accounts are not either authentic or secure" are not correct. As submitted in the preceding paragraphs, RBI has issued detailed instructions to banks about the norms to be followed while opening bank accounts,

24. With reference to the averments made in paragraph 46 of the petition, the allegations against this Respondent are totally false, misleading and quoted out of context with an aim to present distorted facts before this Hon'ble Court. It is submitted that though RBI has no control over the process of Aadhaar enrollment, Master Circular issued by RBI in this regard makes it clear that no account should be opened by banks, without the proper KYC process.

25. With reference to the averments made in paragraphs 47-50 of the Writ Petition, Respondent No. 4 has no comments to offer.

REPLY TO GROUNDS

(i) With reference to the Ground (a) of the Writ Petition, it is submitted that Aadhaar is one of the officially valid documents accepted as proof of identity and address for opening a bank account. RBI has issued detailed instructions regarding operation of money mule accounts and has advised banks that such mule accounts can be minimised if banks follow the guidelines on opening of accounts and monitoring of transactions contained in the Master Circular dated July 1, 2014 issued by Reserve Bank. It is submitted that detailed instructions on monitoring of transactions have also been issued to the banks by Reserve Bank. It has been clarified by the answering Respondent in its circular DBOD.AML.BC. No. 44 /14.01.001/2013-14 dated September 2, 2013, that e-KYC service of UIDAI was accepted as a valid process for KYC verification under Prevention of Money Laundering

(Maintenance of Records) Rules, 2005. It is further specified in Para 2 of the circular that while using e-KYC service of UIDAI, the individual user has to authorize the UIDAI, by explicit consent, to release her or his identity/address through biometric authentication to the bank branches/business correspondents (BCs).

(ii) With reference to the averments made under Grounds (b), (c) (d),(e)and (f), of the Writ Petition, the answering Respondent has no comments to offer.

(iii) With reference to the averments made under Ground (g) it is submitted that the answering Respondent has not issued any instructions to either do away with identification and verification of account holders or declare Aadhaar as sole document for KYC.

(iv) With reference to the averments made under Grounds (h), (i), and (j) of the Writ Petition, the answering Respondent has no comments to offer.

(v) With reference to the averments made under Ground (k), the allegations made against this Respondent are denied. It is reiterated that the answering Respondent has not issued any instructions as such to either do away with identification and verification of account holders or declare Aadhaar as a sole document for KYC.

(vi) With reference to the averments made under Grounds (l), (m) and (n), the answering Respondent has no comments to offer.

(vii) The averments made under Ground (o) of the Writ Petition are wrong. The petitioner is put to strict proof of the same.

(viii) With reference to the averments made under Ground (p) of the Writ Petition, it is reiterated that the answering Respondent has advised banks that Aadhaar is one of the officially valid documents that can be accepted as a 'proof of identity'. Further, banks were also advised not to open an account where the bank is unable to apply appropriate customer due diligence measures, i.e., bank is unable to verify the identity and /or obtain documents required as per the risk categorisation due to non-cooperation of the customer or non-reliability of the data/information furnished to the bank. Bank may also consider closing an existing account under similar circumstances. Similarly, to monitor the operations in an account and mitigate the risks involved, the Master Circular contains instructions for risk management which states that "Ongoing monitoring is an essential element of effective KYC procedures. Banks can effectively control and reduce their risk only if they have an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. It is submitted that the banks have been advised to pay special attention to transactions that involve large amounts of cash, inconsistent with the normal and expected activity of the customer. It is further submitted that e-KYC service of UIDAI was accepted as a valid process for KYC verification under Prevention of Money Laundering (Maintenance of Records) Rules, 2005 and while using e-KYC service of UIDAI, the individual user has to authorize the UIDAI, by explicit consent, to release her or his identity/address through biometric authentication to the bank branches/business correspondents (BCs). It is submitted that the siphoning of funds could take place in any sort of accounts and it is not restricted to accounts opened on the basis of Aadhaar.

(ix) With reference to the averments made under Ground (q) of the Writ Petition, the answering Respondent has no comments to offer.

(x) With reference to the statements made under Ground (r) and (s) of the Writ Petition, the petitioner is put to strict proof.

In the premises, it is humbly prayed that the Petitioner is not entitled to any relief as prayed for or otherwise against the Respondent No.4 and the Writ Petition therefore deserves to be dismissed with costs.

SOLEMNLY AFFIRMED AT NEW DELHI
THIS THE 20th DAY OF JULY, 2015. DEPONENT

VERIFICATION:

I, the deponent above named, do hereby verify that the statements of facts contained in this affidavit are true and correct to the best of my knowledge and nothing material has been concealed.

Verified at New Delhi, this the 20th day of July, 2015.

DEPONENT

ANN.R-III

22

भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA
www.rbi.org.in

RBI/ 2014-15/70
DBOD. AML. BC. No.22/14.01.001/2014-15

July 1, 2014
Ashadha 10, 1936(saka)

The Chairpersons/Chief Executive Officers
All Scheduled Commercial Banks (excluding RRBs) / All India Financial Institutions/ Local Area Banks

Madam/Dear Sir,

Master Circular – Know Your Customer (KYC) norms / Anti-Money Laundering (AML) standards/Combating of Financing of Terrorism (CFT)/Obligation of banks under PMLA, 2002

Please refer to our Master Circular DBOD.AML.BC.No.24/ 14.01.001 / 13 –14 dated July 01, 2013 consolidating instructions/guidelines issued to banks till June 30, 2013 on Know Your Customer (KYC) norms /Anti-Money Laundering (AML) standards/Combating of Financing of Terrorism (CFT)/Obligation of banks under PMLA, 2002. This Master Circular is a consolidation of the instructions on Know Your Customer (KYC) norms /Anti-Money Laundering (AML) standards/Combating of Financing of Terrorism (CFT)/Obligation of banks under PMLA, 2002 issued up to June 30, 2014.

2. The Master Circular has been placed on the RBI website:

(http://www.rbi.org.in)

Yours faithfully,

(Lily Vadera)
Chief General Manager

बैंकिंग परिचालन और विकास विभाग, केंद्रीय कार्यालय, केंद्रीय कार्यालय भवन, 13वीं मंजिल, शहीद भगत सिंह मार्ग, मुंबई - 400 001
फोन: 022-22701203, फैक्स: 022-22701239, ईमेल-: cgmicdbodco@rbi.org.in, वेबसाइट: www.rbi.org.in
Department of Banking Operations & Development, Central Office, Central Office Building, 13th Floor, Shahid Bhagat Singh Marg, Fort, Mumbai – 400 001
Phone : 022-22701203, Fax : 022-22701239, E-mail : cgmicdbodco@rbi.org.in, Website : www.rbi.org.in

हिंदी आसान है, इसका प्रयोग बढ़ाइए

"Caution: RBI never sends mails, SMSs or makes calls asking for personal information like bank account details, passwords, etc. It never keeps or offers funds to anyone. Please do not respond in any manner to such offers."

Master Circular on Know Your Customer (KYC) norms/Anti-Money Laundering (AML) standards/Combating of Financing of Terrorism (CFT)/Obligation of banks under Prevention of Money Laundering Act, (PMLA), 2002

Purpose

Banks were advised to follow certain customer identification procedure for opening of accounts and monitoring transactions of a suspicious nature for the purpose of reporting it to appropriate authority. These 'Know Your Customer' guidelines have been revisited in the context of the Recommendations made by the Financial Action Task Force (FATF) on Anti Money Laundering (AML) standards and on Combating Financing of Terrorism (CFT). Detailed guidelines based on the Recommendations of the Financial Action Task Force and the paper issued on Customer Due Diligence (CDD) for banks by the Basel Committee on Banking Supervision, with indicative suggestions wherever considered necessary, have been issued. Banks have been advised to ensure that a proper policy framework on 'Know Your Customer' and Anti-Money Laundering measures is formulated with the approval of their Board and put in place.

2. This Master Circular aims at consolidating all the instructions/guidelines issued by RBI on Know Your Customer (KYC) norms/Anti-Money Laundering (AML) standards/Combating Financing of Terrorism (CFT)/Obligations of banks under PMLA, 2002. The Master Circular has been placed on the RBI website (http://www.rbi.org.in).

Previous instructions

A list of circulars issued in this regard is given in Annex – IV

Application

i) The instructions, contained in the master circular, are applicable to All India Financial Institutions, all scheduled commercial banks (excluding RRBs) and Local Area Banks.

ii) These guidelines are issued under Section 35A of the Banking Regulation Act, 1949 and Rule 7 of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005. Any contravention thereof or non-compliance shall attract penalties under Banking Regulation Act.

iii) This Master Circular consolidates all the circulars issued on the subject up to June 30, 2014.

25

Index

26

27

1. Introduction

1.1. Know Your Customer (KYC) Norms/Anti-Money Laundering (AML) Measures/Combating of Financing of Terrorism (CFT)/Obligations of banks under PMLA, 2002

The objective of KYC/AML/CFT guidelines is to prevent banks from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities. KYC procedures also enable banks to know/understand their customers and their financial dealings better which in turn help them manage their risks prudently.

1.2. Definition of Customer

For the purpose of KYC policy, a 'Customer' is defined as:

- a person or entity that maintains an account and/or has a business relationship with the bank;
- one on whose behalf the account is maintained (i.e. the beneficial owner). [Ref: Government of India Notification dated February 12, 2010 - Rule 9, sub-rule (1A) of PMLA Rules - 'Beneficial Owner' means the natural person who ultimately owns or controls a client and or the person on whose behalf a transaction is being conducted, and includes a person who exercise ultimate effective control over a juridical person]
- beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law, and
- any person or entity connected with a financial transaction which can pose significant reputational or other risks to the bank, say, a wire transfer or issue of a high value demand draft as a single transaction.

2. Guidelines

2.1. General

i) Banks should keep in mind that the information collected from the customer for the purpose of opening of account is to be treated as confidential and details thereof are not to be divulged for cross selling or any other like purposes. Banks should, therefore, ensure that information

28

sought from the customer is relevant to the perceived risk, is not intrusive, and is in conformity with the guidelines issued in this regard. Any other information from the customer should be sought separately with his/her consent and after opening the account

ii) Banks should ensure that any remittance of funds by way of demand draft, mail/telegraphic transfer or any other mode and issue of travellers' cheques for value of Rupees fifty thousand and above is effected by debit to the customer's account or against cheques and not against cash payment

iii) With effect from April 1, 2012, banks should not make payment of cheques/drafts/pay orders/banker's cheques bearing that date or any subsequent date, if they are presented beyond the period of three months from the date of such instrument.

iv) Banks should ensure that the provisions of Foreign Contribution (Regulation) Act, 2010, wherever applicable, are strictly adhered to.

2.2. KYC Policy

Banks should frame their KYC policies incorporating the following four key elements:

i) Customer Acceptance Policy;

ii) Customer Identification Procedures;

iii) Monitoring of Transactions; and

iv) Risk Management.

2.3. Customer Acceptance Policy (CAP)

a) Every bank should develop a clear Customer Acceptance Policy laying down explicit criteria for acceptance of customers. The Customer Acceptance Policy must ensure that explicit guidelines are in place on the following aspects of customer relationship in the bank.

i) No account is opened in anonymous or fictitious/benami name.

[Ref: Government of India Notification dated June 16, 2010 Rule 9, sub-rule (1C) - Banks should not allow the opening of or keep any

anonymous account or accounts in fictitious name or account on behalf of other persons whose identity has not been disclosed or cannot be verified].

ii) Parameters of risk perception are clearly defined in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status etc. to enable categorisation of customers into low, medium and high risk (banks may choose any suitable nomenclature viz. level I, level II and level III). Customers requiring very high level of monitoring, e.g. Politically Exposed Persons (PEPs) may, if considered necessary, be categorised even higher;

iii) Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of PML Act, 2002 and instructions/guidelines issued by Reserve Bank from time to time;

iv) Not to open an account where the bank is unable to apply appropriate customer due diligence measures, i.e., bank is unable to verify the identity and /or obtain documents required as per the risk categorisation due to non-cooperation of the customer or non-reliability of the data/information furnished to the bank. Bank may also consider closing an existing account under similar circumstances. It is, however, necessary to have suitable built in safeguards to avoid harassment of the customer. For example, decision by a bank to close an account should be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision.

v) Circumstances, in which a customer is permitted to act on behalf of another person/entity, should be clearly spelt out in conformity with the established law and practice of banking as there could be occasions when an account is operated by a mandate holder or where an account is opened by an intermediary in fiduciary capacity and

30

vi) Necessary checks before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organisations etc.

b) Banks should prepare a profile for each new customer based on risk categorisation. The customer profile may contain information relating to customer's identity, social/financial status, nature of business activity, information about his clients' business and their location etc. The nature and extent of due diligence will depend on the risk perceived by the bank. However, while preparing customer profile banks should take care to seek only such information from the customer, which is relevant to the risk category and is not intrusive. The customer profile is a confidential document and details contained therein should not be divulged for cross selling or any other purposes.

c) For the purpose of risk categorisation, individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, may be categorised as low risk. Illustrative examples of low risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government Departments and Government owned companies, regulators and statutory bodies etc. In such cases, the policy may require that only the basic requirements of verifying the identity and location of the customer are to be met. Customers that are likely to pose a higher than average risk to the bank should be categorised as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile, etc. Banks should apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear. In view of the risks involved in cash intensive businesses, accounts of

bullion dealers (including sub-dealers) & jewelers should also be categorized by banks as 'high risk' requiring enhanced due diligence. Other examples of customers requiring higher due diligence include (a) nonresident customers; (b) high net worth individuals; (c) trusts, charities, NGOs and organizations receiving donations; (d) companies having close family shareholding or beneficial ownership; (e) firms with 'sleeping partners'; (f) politically exposed persons (PEPs) of foreign origin, customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner; (g) non-face to face customers and (h) those with dubious reputation as per public information available etc. However, NPOs/NGOs promoted by United Nations or its agencies may be classified as low risk customers.

d) In addition to what has been indicated above, banks/FIs should take steps to identify and assess their ML/TF risk for customers, countries and geographical areas as also for products/ services/ transactions/delivery channels. Banks/FIs should have policies, controls and procedures, duly approved by their boards, in place to effectively manage and mitigate their risk adopting a risk-based approach. As a corollary, banks would be required to adopt enhanced measures for products, services and customers with a medium or high risk rating. In this regard, banks may use for guidance in their own risk assessment, a Report on Parameters for Risk-Based Transaction Monitoring (RBTM) dated March 30, 2011 which was issued by Indian Banks' Association as a supplement to their guidance note on Know Your Customer (KYC) norms / Anti-Money Laundering (AML) standards issued in July 2009. The IBA guidance also provides an indicative list of high risk customers, products, services and geographies.

e) It is important to bear in mind that the adoption of customer acceptance policy and its implementation should not become too restrictive and must not result in denial of banking services to general public, especially to those, who are financially or socially disadvantaged.

32

2.4. Customer Identification Procedure (CIP)

a) The policy approved by the Board of banks should clearly spell out the Customer Identification Procedure to be carried out at different stages, i.e., while establishing a banking relationship; carrying out a financial transaction or when the bank has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data. Customer identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information. Banks need to obtain sufficient information necessary to establish, to their satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of banking relationship. Being satisfied means that the bank must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place. Such risk-based approach is considered necessary to avoid disproportionate cost to banks and a burdensome regime for the customers. Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate etc.). For customers that are natural persons, the banks should obtain sufficient identification data to verify the identity of the customer, his address/location, and also his recent photograph. For customers that are legal persons or entities, the bank should (i) verify the legal status of the legal person/entity through proper and relevant documents; (ii) verify that any person purporting to act on behalf of the legal person/entity is so authorised and identify and verify the identity of that person; (iii) understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person.

b) Banks may seek 'mandatory' information required for KYC purpose which the customer is obliged to give while opening an account or during periodic updation. Other 'optional' customer details/additional information, if required may be obtained separately after the account is opened only with the explicit

consent of the customer. The customer has a right to know what is the information required for KYC that she/he is obliged to give, and what is the additional information sought by the bank that is optional. Further, it is reiterated that banks should keep in mind that the information (both 'mandatory' – before opening the account as well as 'optional'- after opening the account with the explicit consent of the customer) collected from the customer is to be treated as confidential and details thereof are not to be divulged for cross selling or any other like purposes.

c) Customer identification requirements in respect of a few typical cases, especially, legal persons requiring an extra element of caution are given in paragraph 2.5 below for guidance of banks. Banks may, however, frame their own internal guidelines based on their experience of dealing with such persons/entities, normal bankers' prudence and the legal requirements as per established practices. If the bank decides to accept such accounts in terms of the Customer Acceptance Policy, the bank should take reasonable measures to identify the beneficial owner(s) and verify his/her/their identity in a manner so that it is satisfied that it knows who the beneficial owner(s) is/are [Ref: Government of India Notification dated June 16, 2010 - Rule 9 sub-rule (1A) of PML Rules].

d) In this connection, a reference may be made to the circular DBOD.AML.BC. No. 71/14.01.001/2012-13 dated January 18, 2013 wherein the procedure for determination of Beneficial Ownership, as advised by Government of India has been specified.

e) The increasing complexity and volume of financial transactions necessitate that customers do not have multiple identities within a bank, across the banking system and across the financial system. This can be achieved by introducing a unique identification code for each customer. The Unique Customer Identification Code (UCIC) will help banks to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable banks to have a better approach to risk profiling of customers. It would also smoothen banking operations for the customers. While some

34

banks already use UCIC for their customers by providing them a relationship number, etc., other banks have not adopted this practice. Banks were therefore, advised to initiate steps for allotting UCIC to all their customers while entering into any new relationships for individual customers to begin with. Existing individual customers were required to be allotted UCIC by end-May 2013. However, in view of difficulties expressed by some banks in implementing UCIC for their customers, for various reasons, and keeping in view the constraints, the time for completing the process of allotting UCIC to existing customers was extended up to March 31, 2014. In this regard a further extension upto **December 31, 2014** has been allowed. Banks have been advised to expedite the procedure and complete the work of allotting UCIC to all the existing individual customers, within the stipulated timeframe. They may chalk out a plan for completing the work and furnish the monthly progress report to their Board. Considering the fact that a period of two years has been allotted for completion of the task, no further extension in this regard would be considered. Further, it is reiterated that UCIC should be allotted to all customers while entering into new relationships.

f) When there are suspicions of money laundering or financing of the activities relating to terrorism or where there are doubts about the adequacy or veracity of previously obtained customer identification data, banks should review the due diligence measures including verifying again the identity of the client and obtaining information on the purpose and intended nature of the business relationship. [Ref: Government of India Notification dated June 16, 2010- Rule 9 sub-rule (1D) of PML Rules].

g) It has been observed that some close relatives, e.g. wife, son, daughter and parents, etc. who live with their husband, father/mother and son, as the case may be, are finding it difficult to open account in some banks as the utility bills required for address verification are not in their name. It is clarified, that in such cases, banks can obtain an identity document and a utility bill of the relative with whom the prospective customer is living along with a declaration from the relative that the said person (prospective customer) wanting to open

an account is a relative and is staying with him/her. Banks can use any supplementary evidence such as a letter received through post for further verification of the address. While issuing operational instructions to the branches on the subject, banks should keep in mind the spirit of instructions issued by the Reserve Bank and avoid undue hardships to individuals who are, otherwise, classified as low risk customers.

h) Norms for furnishing proof of address have been relaxed to allow submitting only one documentary proof of address (either current or permanent) while opening a bank account or while undergoing periodic updation. In case the address mentioned as per 'proof of address' undergoes a change, fresh proof of address may be submitted to the branch within a period of six months. In case the proof of address furnished by the customer is not the local address or address where the customer is currently residing, the bank may take a declaration of the local address on which all correspondence will be made by the bank with the customer. No proof is required to be submitted for such address for correspondence/local address. This address may be verified by the bank through 'positive confirmation' such as acknowledgment of receipt of (i) letter, cheque books, ATM cards; (ii) telephonic conversation; (iii) visits; etc. In the event of change in this address due to relocation or any other reason, customers may intimate the new address for correspondence to the bank within two weeks of such a change.

i) Some banks insist on opening of fresh accounts by customers when customers approach them for transferring their account from one branch of the bank to another branch of the same bank. Banks are advised that KYC once done by one branch of the bank should be valid for transfer of the account within the bank as long as full KYC has been done for the concerned account. The customer should be allowed to transfer his account from one branch to another branch without restrictions. Banks may transfer existing accounts at the transferor branch to the transferee branch without insisting on fresh proof of address and on the basis of a self-declaration from the account holder about his/her current address.

36

j) Banks should carry out periodical updation of KYC information of every customer, which may include the following:

   i) Full KYC exercise may be done at least every two years for high risk customers, every eight years for medium risk customers and every ten years for low risk customers. Full KYC may include all measures for confirming identity and address and other particulars of the customer that the bank may consider reasonable and necessary based on the risk profile of the customer.

   ii) Positive confirmation (obtaining KYC related updates through e-mail/ letter/ telephonic conversation/ forms/ interviews/ visits, etc.), may be completed at least every two years for medium risk and at least every three years for low risk individuals and entities.

   iii) Fresh photographs to be obtained from minor customer on becoming major.

   iv) The time limits prescribed above would apply from the date of opening of the account/ last verification of KYC.

k) An indicative list of the nature and type of documents/information that may be may be relied upon for customer identification is given in Annex-I to this Master Circular.

l) If the address on the document submitted for identity proof by the prospective customer is same as that declared by him/her in the account opening form, the document may be accepted as a valid proof of both identity and address.

m) A rent agreement indicating the address of the customer duly registered with State Government or similar registration authority may also be accepted as a proof of address.

n) It has been brought to our notice that the said indicative list furnished in Annex - I, is being treated by some banks as an exhaustive list as a result of which a section of public is being denied access to banking services. Banks are, therefore, advised to take a review of their extant internal instructions in this regard.

37

2.5. Customer Identification Requirements – Indicative Guidelines

a) **Walk-in Customers**

In case of transactions carried out by a non-account based customer, that is a walk-in customer, where the amount of transaction is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, the customer's identity and address should be verified. However, if a bank has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs.50,000/- the bank should verify the identity and address of the customer and also consider filing a suspicious transaction report (STR) to FIU-IND.

NOTE: **In terms of Clause (b) (ii) of sub-Rule (1) of Rule 9 of the PML Rules, 2005 banks and financial institutions are required to verify the identity of the customers for <u>all</u> international money transfer operations**

b) **Salaried Employees**

In case of salaried employees, it is clarified that with a view to containing the risk of fraud, banks should rely on certificate/letter of identity and/or address issued only from corporate and other entities of repute and should be aware of the competent authority designated by the concerned employer to issue such certificate/letter. Further, <u>in addition</u> to the certificate/letter issued by the employer, banks should insist on at least one of the officially valid documents as provided in the Prevention of Money Laundering Rules (viz. passport, driving licence, PAN Card, Voter's Identity card, etc.) or utility bills for KYC purposes for opening bank accounts of salaried employees of corporate and other entities.

c) **Trust/Nominee or Fiduciary Accounts**

There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. Banks should determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, banks should insist on receipt of satisfactory

38

evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place. While opening an account for a trust, banks should take reasonable precautions to verify the identity of the trustees and the settlors of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories. Beneficiaries should be identified when they are defined. In the case of a 'foundation', steps should be taken to verify the founder managers/ directors and the beneficiaries, if defined.

d) Accounts of companies and firms

Banks need to be vigilant against business entities being used by individuals as a 'front' for maintaining accounts with banks. Banks should examine the control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management. These requirements may be moderated according to the risk perception e.g. in the case of a public company it will not be necessary to identify all the shareholders.

e) Client accounts opened by professional intermediaries

i) When the bank has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client must be identified. Banks may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. Banks also maintain 'pooled' accounts managed by lawyers/chartered accountants or stockbrokers for funds held 'on deposit' or 'in escrow' for a range of clients. Where funds held by the intermediaries are not co-mingled at the bank and there are 'sub-accounts', each of them attributable to a beneficial owner, all the beneficial owners must be identified. Where such funds are co-mingled at the bank, the bank should still look through to the beneficial owners. Where the banks rely on the 'customer due diligence' (CDD) done by an intermediary, they should satisfy themselves that the intermediary is regulated and supervised and has adequate systems in place to comply

39

with the KYC requirements. It should be understood that the ultimate responsibility for knowing the customer lies with the bank.

ii) Under the extant AML/CFT framework, therefore, it is not possible for professional intermediaries like Lawyers and Chartered Accountants, etc. who are bound by any client confidentiality that prohibits disclosure of the client details, to hold an account on behalf of their clients. It is reiterated that banks should not allow opening and/or holding of an account on behalf of a client/s by professional intermediaries, like Lawyers and Chartered Accountants, etc., who are unable to disclose true identity of the owner of the account/funds due to any professional obligation of customer confidentiality. Further, any professional intermediary who is under any obligation that inhibits bank's ability to know and verify the true identity of the client on whose behalf the account is held or beneficial ownership of the account or understand true nature and purpose of transaction/s, should not be allowed to open an account on behalf of a client.

f) **Accounts of Politically Exposed Persons (PEPs) resident outside India**

i) Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. Banks should gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on the person in the public domain. Banks should verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. The decision to open an account for a PEP should be taken at a senior level which should be clearly spelt out in Customer Acceptance Policy. Banks should also subject such accounts to enhanced monitoring on an ongoing basis. The above norms may also

40

be applied to the accounts of the family members or close relatives of PEPs.

ii) In the event of an existing customer or the beneficial owner of an existing account, subsequently becoming a PEP, banks should obtain senior management approval to continue the business relationship and subject the account to the CDD measures as applicable to the customers of PEP category including enhanced monitoring on an ongoing basis. These instructions are also applicable to accounts where a PEP is the ultimate beneficial owner.

iii) Further, banks should have appropriate ongoing risk management procedures for identifying and applying enhanced CDD to PEPs, customers who are close relatives of PEPs, and accounts of which a PEP is the ultimate beneficial owner.

g) Accounts of non-face-to-face customers

With the introduction of telephone and electronic banking, increasingly accounts are being opened by banks for customers without the need for the customer to visit the bank branch. In the case of non-face-to-face customers, apart from applying the usual customer identification procedures, there must be specific and adequate procedures to mitigate the higher risk involved. Certification of all the documents presented should be insisted upon and, if necessary, additional documents may be called for. In such cases, banks may also require the first payment to be effected through the customer's account with another bank which, in turn, adheres to similar KYC standards. In the case of cross-border customers, there is the additional difficulty of matching the customer with the documentation and the bank may have to rely on third party certification/introduction. In such cases, it must be ensured that the third party is a regulated and supervised entity and has adequate KYC systems in place.

h) Accounts of proprietary concerns

Apart from following the extant guidelines on customer identification procedure as applicable to the proprietor, banks should call for and verify the following documents before opening of accounts in the name of a proprietary concern:

41

Proof of the name, address and activity of the concern, like registration certificate (in the case of a registered concern), certificate/licence issued by the Municipal authorities under Shop & Establishment Act, sales and income tax returns, CST/VAT certificate, certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities, Licence issued by the Registering authority like Certificate of Practice issued by Institute of Chartered Accountants of India, Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food and Drug Control Authorities, registration/licensing document issued in the name of the proprietary concern by the Central Government or State Government Authority/Department. Banks may also accept IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT, the complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities and utility bills such as electricity, water, and landline telephone bills in the name of the proprietary concern as required documents for opening of bank accounts of proprietary concerns. .

Any two of the above documents would suffice. These documents should be in the name of the proprietary concern.

j) **Procedure to be followed in respect of foreign students:**

Banks may follow the following procedure for foreign students studying in India.

i) Banks may open a Non Resident Ordinary (NRO) bank account of a foreign student on the basis of his/her passport (with appropriate visa & immigration endorsement) which contains the proof of identity and address in the home country along with a photograph and a letter offering admission from the educational institution.

ii) Within a period of 30 days of opening the account, the foreign student should submit to the branch where the account is opened, a valid address proof giving local address, in the form of a rent agreement or a letter from the educational institution as a proof of living in a facility

42

provided by the educational institution. Banks should not insist on the landlord visiting the branch for verification of rent documents and alternative means of verification of local address may be adopted by banks.

iii) During the 30 days period, the account should be operated with a condition of allowing foreign remittances not exceeding USD 1,000 into the account and a cap of monthly withdrawal to Rs. 50,000/-, pending verification of address.

iv) On submission of the proof of current address, the account would be treated as a normal NRO account, and will be operated in terms of instructions contained in the Reserve Bank of India's instructions on Non-Resident Ordinary Rupee (NRO) Account, and the provisions of Schedule 3 of FEMA Notification 5/2000 RB dated May 3, 2000.

v) Students with Pakistani nationality will need prior approval of the Reserve Bank for opening the account.

2.6. Selling Third party products

When banks sell third party products as agents, the responsibility for ensuring compliance with KYC/AML/CFT regulations lies with the third party. However, to mitigate reputational risk to bank and to enable a holistic view of a customer's transactions, banks are advised as follows:

(a) Even while selling third party products as agents, banks should verify the identity and address of the walk-in customer.

(b) Banks should also maintain transaction details with regard to sale of third party products and related records for a period and in the manner prescribed in paragraph 2.24 below.

(c) Bank's AML software should be able to capture, generate and analyse alerts for the purpose of filing CTR/STR in respect of transactions relating to third party products with customers including walk-in customers.

(d) Sale of third party products by banks as agents to customers, including walk-in customers, for Rs.50,000 and above must be (a) by debit to customers' account or against cheques and (b) obtention & verification of the PAN given

43

by the account based as well as walk-in customers. This instruction would also apply to sale of banks' own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for Rs. 50,000/- and above.

2.7. Due Diligence in correspondent banking relationship

Some commercial banks have arrangements with co-operative banks wherein the latter open current accounts with the commercial banks and use the cheque book facility to issue 'at par' cheques to their constituents and walk-in- customers for facilitating their remittances and payments. Since the 'at par' facility offered by commercial banks to co-operative banks is in the nature of correspondent banking arrangements, banks should monitor and review such arrangements to assess the risks including credit risk and reputational risk arising therefrom. For this purpose, banks should retain the right to verify the records maintained by the client cooperative banks/ societies for compliance with the extant instructions on KYC and AML under such arrangements.

2.8. Simplified KYC norms for Foreign Portfolio Investors (FPIs)

In terms of Rule 9 (14)(i) of the PML Rules, simplified norms have been prescribed for those FPIs who have been duly registered in accordance with SEBI guidelines and have undergone the required KYC due diligence/verification prescribed by SEBI through a Custodian/Intermediary regulated by SEBI. Such eligible/registered FPIs may approach a bank for opening a bank account for the purpose of investment under Portfolio Investment Scheme (PIS) for which KYC documents prescribed by the Reserve Bank (as detailed in Annex II of the circular DBOD.AML.BC.No.103/14.01.001/2013-14 dated April 3, 2014) would be required. For this purpose, banks may rely on the KYC verification done by the third party (i.e. the Custodian/SEBI Regulated Intermediary) subject to the conditions laid down in Rule 9 (2) [(a) to (e)] of the Rules.

2.9. Small Accounts

In terms of Government of India, Notification No. 14/2010/F.No.6/2/2007-E.S dated December 16, 2010, (Annex - III a 'small account' means a savings account in a banking company where-

44

i.the aggregate of all credits in a financial year does not exceed rupees one lakh;

ii.the aggregate of all withdrawals and transfers in a month does not exceed rupees ten thousand; and

iii. the balance at any point of time does not exceed rupees fifty thousand.

(a) A 'small account' may be opened on the basis of a self-attested photograph and affixation of signature or thumb print. Such accounts may be opened and operated subject to the following conditions:

i) the designated officer of the bank, while opening the small account, certifies under his signature that the person opening the account has affixed his signature or thumb print, as the case may be, in his presence;

ii) a small account shall be opened only at Core Banking Solution linked bank branches or in a branch where it is possible to manually monitor and ensure that foreign remittances are not credited to the account and that the stipulated limits on monthly and annual aggregate of transactions and balance in such accounts are not breached, before a transaction is allowed to take place;

iii) a small account shall remain operational initially for a period of twelve months, and thereafter for a further period of twelve months if the holder of such an account provides evidence before the banking company of having applied for any of the officially valid documents within twelve months of the opening of the said account, with the entire relaxation provisions to be reviewed in respect of the said account after twenty four months;

iv) a small account shall be monitored and when there is suspicion of money laundering or financing of terrorism or other high risk scenarios, the identity of customer shall be established through the production of "officially valid documents"; and

v) foreign remittance shall not be allowed to be credited into a small account unless the identity of the customer is fully established through the production of "officially valid documents".

45

2.10. Officially Valid Documents under Government of India notifications

(a) The notifications further state that job card issued by NREGA duly signed by an officer of the State Government and the letters issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number can now be accepted as an 'Officially Valid Document'.

(b) E-KYC service of Unique Identification Authority of India (UIDAI) may be accepted as a valid process for KYC verification under the PML Rules. The information containing demographic details and photographs made available from UIDAI as a result of e-KYC process may be treated as an 'Officially Valid Document'. However, the individual user has to authorize to UIDAI, by explicit consent, to release her or his identity/address through biometric authentication to the bank branches/business correspondents.

(c) Further, e-Aadhaar downloaded from UIDAI website may be accepted as an officially valid document subject to the following:

i. If the prospective customer knows only his/her Aadhaar number, the bank may print the prospective customer's e-Aadhaar letter in the bank directly from the UIDAI portal; or adopt e-KYC procedure as mentioned in paragraph (b) above.

ii. If the prospective customer carries a copy of the e-Aadhaar downloaded elsewhere, the bank may print the prospective customer's e-Aadhaar letter in the bank directly from the UIDAI portal; or adopt e-KYC procedure as mentioned in paragraph (b) above; or confirm identity and address of the resident through simple authentication service of UIDAI.

2.11. Operation of Bank Accounts & Money Mules

a) It has been brought to our notice that "Money Mules" can be used to launder the proceeds of fraud schemes (*e.g.*, phishing and identity theft) by criminals who gain illegal access to deposit accounts by recruiting third parties to act as "money mules." In some cases these third parties may be innocent while in others they may be having complicity with the criminals.

b) In a money mule transaction, an individual with a bank account is recruited to receive cheque deposits or wire transfers and then transfer these funds to

46

accounts held on behalf of another person or to other individuals, minus a certain commission payment. Money mules may be recruited by a variety of methods, including spam e-mails, advertisements on genuine recruitment web sites, social networking sites, instant messaging and advertisements in newspapers. When caught, these money mules often have their bank accounts suspended, causing inconvenience and potential financial loss, apart from facing likely legal action for being part of a fraud. Many a times the address and contact details of such mules are found to be fake or not up to date, making it difficult for enforcement agencies to locate the account holder.

c) The operations of such mule accounts can be minimised if banks follow the guidelines on opening of accounts and monitoring of transactions contained in this Master Circular. Banks are, therefore, advised to strictly adhere to the guidelines on KYC/AML/CFT issued from time to time and to those relating to periodical updation of customer identification data after the account is opened and also to monitoring of transactions in order to protect themselves and their customers from misuse by such fraudsters.

2.12. Bank No Longer Knows the True Identity

In the circumstances when a bank believes that it would no longer be satisfied that it knows the true identity of the account holder, the bank should also file an STR with FIU-IND.

2.13. Monitoring of Transactions

a) Ongoing monitoring is an essential element of effective KYC procedures. Banks can effectively control and reduce their risk only if they have an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity of the account. Banks should pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. Banks may prescribe threshold limits for a particular category of accounts and pay particular attention to the transactions which exceed these limits. Transactions that

47

involve large amounts of cash inconsistent with the normal and expected activity of the customer should particularly attract the attention of the bank. Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being 'washed' through the account. High-risk accounts have to be subjected to intensified monitoring. Every bank should set key indicators for such accounts, taking note of the background of the customer, such as the country of origin, sources of funds, the type of transactions involved and other risk factors. High risk associated with accounts of bullion dealers (including sub-dealers) & jewelers should be taken into account by banks to identify suspicious transactions for filing Suspicious Transaction Reports (STRs) to Financial Intelligence Unit- India (FIU-IND). Banks should put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures. Such review of risk categorisation of customers should be carried out at a periodicity of **not less** than once in six months.

b) It has come to our notice that accounts of Multi-level Marketing (MLM) Companies were misused for defrauding public by luring them into depositing their money with the MLM company by promising a high return. Such depositors are assured of high returns and issued post-dated cheques for interest and repayment of principal. So long as money keeps coming into the MLM company's account from new depositors, the cheques are honoured but once the chain breaks, all such post-dated instruments are dishonoured. This results in fraud on the public and is a reputational risk for banks concerned. Further, banks should closely monitor the transactions in accounts of marketing firms. In cases where a large number of cheque books are sought by the company, there are multiple small deposits (generally in cash) across the country in one bank account and where a large number of cheques are issued bearing similar amounts/dates, the bank should carefully analyse such data and in case they find such unusual operations in accounts, the matter should be immediately reported to Reserve Bank and other appropriate

48

authorities such as Financial Intelligence Unit India (FIU-Ind) under Department of Revenue, Ministry of Finance.

c) Banks should exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge of the client, his business and risk profile and where necessary, the source of funds [Ref: Government of India Notification dated June 16, 2010 -Rule 9, sub-rule (1B)]

d) The risk categorization of customers as also compilation and periodic updation of customer profiles and monitoring and closure of alerts in accounts by banks are extremely important for effective implementation of KYC/AML/CFT measures. It is, however, observed that there are laxities in effective implementation of the Reserve Bank's guidelines in this area, leaving banks vulnerable to operational risk. Banks should, therefore, ensure compliance with the regulatory guidelines on KYC/AML/CFT both in letter and spirit. Accordingly, banks were advised to complete the process of risk categorization and compiling/updating profiles of all of their existing customers in a time-bound manner, by end-March 2013.

2.14. Closure of accounts

Where the bank is unable to apply appropriate KYC measures due to non-furnishing of information and /or non-cooperation by the customer, the bank should consider closing the account or terminating the banking/business relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Such decisions need to be taken at a reasonably senior level.

2.15. Risk Management

a) The Board of Directors of the bank should ensure that an effective KYC programme is put in place by establishing appropriate procedures and ensuring their effective implementation. It should cover proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility should be explicitly allocated within the bank for ensuring that the bank's policies and procedures are implemented

49

effectively. Banks should, in consultation with their boards, devise procedures for creating risk profiles of their existing and new customers, assess risk in dealing with various countries, geographical areas and also the risk of various products, services, transactions, delivery channels, etc. Banks' policies should address effectively managing and mitigating these risks adopting a risk-based approach as discussed in Para 2.3 (d) above.

b) Banks' internal audit and compliance functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures. As a general rule, the compliance function should provide an independent evaluation of the bank's own policies and procedures, including legal and regulatory requirements. Banks should ensure that their audit machinery is staffed adequately with individuals who are well-versed in such policies and procedures. Concurrent/ Internal Auditors should specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard. The compliance in this regard should be put up before the Audit Committee of the Board on quarterly intervals.

2.16. Introduction of New Technologies – Credit Cards/Debit Cards/ Smart Cards/Gift Cards

Banks should pay special attention to any money laundering threats that may arise from new or developing technologies including internet banking that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. Many banks are engaged in the business of issuing a variety of Electronic Cards that are used by customers for buying goods and services, drawing cash from ATMs, and can be used for electronic transfer of funds. Banks are required to ensure full compliance with all KYC/AML/CFT guidelines issued from time to time, in respect of add-on/ supplementary cardholders also. Further, marketing of credit cards is generally done through the services of agents. Banks should ensure that appropriate KYC procedures are duly applied before issuing the cards to the customers. It is also desirable that agents are also subjected to KYC measures.

2.17. Combating Financing of Terrorism

In terms of PMLA Rules, suspicious transaction should include, *inter alia,*

a. Transactions, which give rise to a reasonable ground of suspicion that these may involve financing of the activities relating to terrorism. Banks are, therefore, advised to develop suitable mechanism through appropriate policy framework for enhanced monitoring of accounts suspected of having terrorist links and swift identification of the transactions and making suitable reports to FIU-Ind on priority.

b. As and when list of individuals and entities, approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs), are received from Government of India, Reserve Bank circulates these to all banks and financial institutions. Banks/Financial Institutions should ensure to update the lists of individuals and entities as circulated by Reserve Bank. The UN Security Council has adopted Resolutions 1988 (2011) and 1989 (2011) which have resulted in splitting of the 1267 Committee's Consolidated List into two separate lists, namely:

   i) **"Al-Qaida Sanctions List"**, which is maintained by the 1267 / 1989 Committee. This list shall include only the names of those individuals, groups, undertakings and entities associated with Al-Qaida. The Updated Al-Qaida Sanctions List is available at http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml

   ii) **"1988 Sanctions List"**, which is maintained by the 1988 Committee. This list consists of names previously included in Sections A ("Individuals associated with the Taliban") and B ("Entities and other groups and undertakings associated with the Taliban") of the Consolidated List. The Updated 1988 Sanctions list is available at http://www.un.org/sc/committees/ 1988/list.shtml

It may be noted that both "Al-Qaida Sanctions List" and "1988 Sanctions List" are to be taken into account for the purpose of implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967.

Banks are advised that before opening any new account it should be ensured that the name/s of the proposed customer does not appear in the lists. Further, banks should scan all existing accounts to ensure that no account is held by or linked

to any of the entities or individuals included in the list. Full details of accounts bearing resemblance with any of the individuals/entities in the list should immediately be intimated to RBI and FIU-IND.

2.18. Freezing of Assets under Section 51A of Unlawful Activities (Prevention) Act, 1967

a) The Unlawful Activities (Prevention) Act, 1967 (UAPA) has been amended by the Unlawful Activities (Prevention) Amendment Act, 2008. Government has issued an Order dated August 27, 2009 detailing the procedure for implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967 relating to the purposes of prevention of, and for coping with terrorist activities. In terms of Section 51A, the Central Government is empowered to freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of or at the direction of the individuals or entities Listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism and prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities Listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism.

b) Banks are required to strictly follow the procedure laid down in the UAPA Order dated August 27, 2009 (Annex II) and ensure meticulous compliance to the Order issued by the Government.

c) On receipt of the list of individuals and entities subject to UN sanctions (referred to as designated lists) from RBI, banks should ensure expeditious and effective implementation of the procedure prescribed under Section 51A of UAPA in regard to freezing/unfreezing of financial assets of the designated individuals/entities enlisted in the UNSCRs and especially, in regard to funds, financial assets or economic resources or related services held in the form of bank accounts.

d) In terms of Para 4 of the Order, in regard to **funds, financial assets or economic resources or related services held in the form of bank**

52

accounts, the RBI would forward the designated lists to the banks requiring them to:

i) Maintain updated designated lists in electronic form and run a check on the given parameters on a regular basis to verify whether individuals or entities listed in the schedule to the Order (referred to as designated individuals/entities) are holding any funds, financial assets or economic resources or related services held in the form of bank accounts with them.

ii) In case, the particulars of any of their customers match with the particulars of designated individuals/entities, the banks shall immediately, not later than 24 hours from the time of finding out such customer, inform full particulars of the funds, financial assets or economic resources or related services held in the form of bank accounts, held by such customer on their books to the Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No.011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on e-mail id: jsis@nic.in

iii) Banks shall also send by post, a copy of the communication mentioned in (ii) above to the UAPA nodal officer of RBI, Chief General Manager, Department of Banking Operations and Development, Central Office, Reserve Bank of India, Anti Money Laundering Division, Central Office Building, 13th Floor, Shahid Bhagat Singh Marg, Fort, Mumbai - 400 001 and also by fax at No.022-22701239. The particulars, apart from being sent by post/fax should necessarily be conveyed on e-mail id: cgmaml@rbi.org.in

iv) Banks shall also send a copy of the communication mentioned in (ii) above to the UAPA nodal officer of the state/UT where the account is held as the case may be and to FIU-India.

v) In case, the match of any of the customers with the particulars of designated individuals/entities is **beyond doubt,** the banks would

prevent designated persons from conducting financial transactions, under intimation to Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No. 011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on e-mail id: jsis@nic.in.

vi) Banks shall also file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions in the accounts covered by paragraph (ii) above, carried through or attempted, as per the prescribed format.

e) **Freezing of financial assets**

i) On receipt of the particulars as mentioned in paragraph d(ii)) above, IS-I Division of MHA would cause a verification to be conducted by the State Police and /or the Central Agencies so as to ensure that the individuals/ entities identified by the banks are the ones listed as designated individuals/entities and the funds, financial assets or economic resources or related services , reported by banks are held by the designated individuals/entities. This verification would be completed within a period not exceeding five working days from the date of receipt of such particulars.

ii) In case, the results of the verification indicate that the properties are owned by or held for the benefit of the designated individuals/entities, an order to freeze these assets under section 51A of the UAPA would be issued within 24 hours of such verification and conveyed electronically to the concerned bank branch under intimation to Reserve Bank of India and FIU-IND.

iii) The order shall take place without prior notice to the designated individuals/entities.

f) **Implementation of requests received from foreign countries under U.N. Security Council Resolution 1373 of 2001.**

i) U.N. Security Council Resolution 1373 obligates countries to freeze without delay the funds or other assets of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities or controlled directly or indirectly

by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds or other assets derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons and entities.

ii) To give effect to the requests of foreign countries under U.N. Security Council Resolution 1373, the Ministry of External Affairs shall examine the requests made by the foreign countries and forward it electronically, with their comments, to the UAPA nodal officer for IS-I Division for freezing of funds or other assets.

iii) The UAPA nodal officer of IS-I Division of MHA, shall cause the request to be examined, within five working days so as to satisfy itself that on the basis of applicable legal principles, the requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances terrorism or a terrorist organization, and upon his satisfaction, request would be electronically forwarded to the nodal officers in RBI. The proposed designee, as mentioned above would be treated as designated individuals/entities.

iv) Upon receipt of the requests from the UAPA nodal officer of IS-I Division, the list would be forwarded to banks and the procedure as enumerated at paragraphs 2.18[(c), (d) and (e)] shall be followed.

v) The freezing orders shall take place without prior notice to the designated persons involved.

g) **Procedure for unfreezing of funds, financial assets or economic resources or related services of individuals/entities inadvertently affected by the freezing mechanism upon verification that the person or entity is not a designated person**

Any individual or entity, if it has evidence to prove that the freezing of funds, financial assets or economic resources or related services, owned/held by them has been inadvertently frozen, they shall move an application giving the requisite evidence, in writing, to the concerned bank. The banks shall inform and forward a copy of the application together with

25

full details of the asset frozen given by any individual or entity informing of the funds, financial assets or economic resources or related services have been frozen inadvertently, to the nodal officer of IS-I Division of MHA as per the contact details given in paragraph (d)(ii) above within two working days. The Joint Secretary (IS-I), MHA, being the nodal officer for (IS-I) Division of MHA, shall cause such verification as may be required on the basis of the evidence furnished by the individual/entity and if he is satisfied, he shall pass an order, within fifteen working days, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant under intimation to the concerned bank. However, if it is not possible for any reason to pass an order unfreezing the assets within fifteen working days, the nodal officer of IS-I Division shall inform the applicant.

h) **Communication of Orders under Section 51A of Unlawful Activities (Prevention) Act.**

All Orders under Section 51A of Unlawful Activities (Prevention) Act, relating to funds, financial assets or economic resources or related services, would be communicated to all banks through RBI.

2.19. Jurisdictions that do not or insufficiently apply the FATF Recommendations

a) Banks are required to take into account risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement. In addition to FATF Statements circulated by Reserve Bank of India from time to time, (latest as on June 30, 2014, being our circular DBOD. AML.No.15245/14.01.001/2013-14 dated March 05, 2014) banks should also consider publicly available information for identifying countries, which do not or insufficiently apply the FATF Recommendations. It is clarified that banks should also give special attention to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF Statements.

b) Banks should examine the background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations. Further, if the transactions have no apparent economic or visible lawful purpose, the background and purpose of such transactions should, as far as possible be examined, and written findings together with all documents should be retained and made available to Reserve Bank/other relevant authorities, on request.

2.20. Correspondent Banking and Shell Bank

a) Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). These services may include cash/funds management, international wire transfers, drawing arrangements for demand drafts and mail transfers, payable-through-accounts, cheques clearing etc. Banks should gather sufficient information to understand fully the nature of the business of the correspondent/respondent bank. Information on the other bank's management, major business activities, level of AML/CFT compliance, purpose of opening the account, identity of any third party entities that will use the correspondent banking services, and regulatory/supervisory framework in the correspondent's/respondent's country may be of special relevance. Similarly, banks should try to ascertain from publicly available information whether the other bank has been subject to any money laundering or terrorist financing investigation or regulatory action. While it is desirable that such relationships should be established only with the approval of the Board, in case the Boards of some banks wish to delegate the power to an administrative authority, they may delegate the power to a committee headed by the Chairman/CEO of the bank while laying down clear parameters for approving such relationships. Proposals approved by the Committee should invariably be put up to the Board at its next meeting for post facto approval. The responsibilities of each bank with whom correspondent banking relationship is established should be clearly documented. In the case

57

of payable-through-accounts, the correspondent bank should be satisfied that the respondent bank has verified the identity of the customers having direct access to the accounts and is undertaking ongoing 'due diligence' on them. The correspondent bank should also ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.

b) **Correspondent relationship with a "Shell Bank"**

Banks should refuse to enter into a correspondent relationship with a "shell bank" (i.e. a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group). Shell banks are not permitted to operate in India. Banks should not enter into relationship with shell banks and before establishing correspondent relationship with any foreign institution, banks should take appropriate measures to satisfy themselves that the foreign respondent institution does not permit its accounts to be used by shell banks. Banks should be extremely cautious while continuing relationships with correspondent banks located in countries with poor KYC standards and countries identified as 'non-cooperative' in the fight against money laundering and terrorist financing. Banks should ensure that their respondent banks have anti money laundering policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts.

2.21. Applicability to branches and subsidiaries outside India

The guidelines contained in this master circular shall apply to the branches and majority owned subsidiaries located abroad, especially, in countries which do not or insufficiently apply the FATF Recommendations, to the extent local laws permit. When local applicable laws and regulations prohibit implementation of these guidelines, the same should be brought to the notice of Reserve Bank. In case there is a variance in KYC/AML standards prescribed by the Reserve Bank and the host country regulators, branches/overseas subsidiaries of banks are required to adopt the more stringent regulation of the two.

58

2.22. Wire Transfer

Banks use wire transfers as an expeditious method for transferring funds between bank accounts. Wire transfers include transactions occurring within the national boundaries of a country or from one country to another. As wire transfers do not involve actual movement of currency, they are considered as rapid and secure method for transferring value from one location to another.

a) The salient features of a wire transfer transaction are as under:
   i) Wire transfer is a transaction carried out on behalf of an originator person (both natural and legal) through a bank by electronic means with a view to making an amount of money available to a beneficiary person at a bank. The originator and the beneficiary may be the same person.
   ii) Cross-border transfer means any wire transfer where the originator and the beneficiary bank or financial institutions are located in different countries. It may include any chain of wire transfers that has at least one cross-border element.
   iii) Domestic wire transfer means any wire transfer where the originator and receiver are located in the same country. It may also include a chain of wire transfers that takes place entirely within the borders of a single country even though the system used to effect the wire transfer may be located in another country.
   iv) The originator is the account holder, or where there is no account, the person (natural or legal) that places the order with the bank to perform the wire transfer.

b) Wire transfer is an instantaneous and most preferred route for transfer of funds across the globe and hence, there is a need for preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds and for detecting any misuse when it occurs. This can be achieved if basic information on the originator of wire transfers is immediately available to appropriate law enforcement and/or prosecutorial authorities in order to assist them in detecting, investigating, prosecuting terrorists or other criminals and

59

tracing their assets. The information can be used by Financial Intelligence Unit - India (FIU-IND) for analysing suspicious or unusual activity and disseminating it as necessary. The originator information can also be put to use by the beneficiary bank to facilitate identification and reporting of suspicious transactions to FIU-IND. Owing to the potential terrorist financing threat posed by small wire transfers, the objective is to be in a position to trace all wire transfers with minimum threshold limits. Accordingly, banks must ensure that all wire transfers are accompanied by the following information:

1. **Cross-border wire transfers**

   i) All cross-border wire transfers must be accompanied by accurate and meaningful originator information.

   ii) Information accompanying cross-border wire transfers must contain the name and address of the originator and where an account exists, the number of that account. In the absence of an account, a unique reference number, as prevalent in the country concerned, must be included.

   iii) Where several individual transfers from a single originator are bundled in a batch file for transmission to beneficiaries in another country, they may be exempted from including full originator information, provided they include the originator's account number or unique reference number as at (ii) above.

2. **Domestic wire transfers**

   i) Information accompanying all domestic wire transfers of Rs.50000/- (Rupees Fifty Thousand) and above must include complete originator information i.e. name, address and account number etc., unless full originator information can be made available to the beneficiary bank by other means.

   ii) If a bank has reason to believe that a customer is intentionally structuring wire transfer to below Rs. 50000/- (Rupees Fifty Thousand) to several beneficiaries in order to avoid reporting or monitoring, the bank must insist on complete customer

identification before effecting the transfer. In case of non-cooperation from the customer, efforts should be made to establish his identity and Suspicious Transaction Report (STR) should be made to FIU-IND.

iii) When a credit or debit card is used to effect money transfer, necessary information as (i) above should be included in the message.

c) **Exemptions**

Interbank transfers and settlements where both the originator and beneficiary are banks or financial institutions would be exempted from the above requirements.

d) **Role of Ordering, Intermediary and Beneficiary banks**

i) **Ordering Bank**

An ordering bank is the one that originates a wire transfer as per the order placed by its customer. The ordering bank must ensure that qualifying wire transfers contain complete originator information. The bank must also verify and preserve the information at least for a period of ten years.

ii)**Intermediary bank**

For both cross-border and domestic wire transfers, a bank processing an intermediary element of a chain of wire transfers must ensure that all originator information accompanying a wire transfer is retained with the transfer. Where technical limitations prevent full originator information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, a record must be kept at least for ten years (as required under Prevention of Money Laundering Act, 2002) by the receiving intermediary bank of all the information received from the ordering bank.

iii) **Beneficiary bank**

A beneficiary bank should have effective risk-based procedures in place to identify wire transfers lacking complete originator information. The lack of complete originator information may be considered as a factor in

61

assessing whether a wire transfer or related transactions are suspicious and whether they should be reported to the Financial Intelligence Unit-India. The beneficiary bank should also take up the matter with the ordering bank if a transaction is not accompanied by detailed information of the fund remitter. If the ordering bank fails to furnish information on the remitter, the beneficiary bank should consider restricting or even terminating its business relationship with the ordering bank.

2.23. Designated Director and Principle Officer

a) **Designated Director**

Banks are required to nominate a Director on their Boards as "Designated Director", as per the provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (Rules), to ensure overall compliance with the obligations under the Act and Rules. The name, designation and address of the Designated Director is to be communicated to the Director, Financial Intelligence Unit – India (FIU-IND).

b) **Principal Officer**

Banks should appoint a senior management officer to be designated as Principal Officer. Banks should ensure that the Principal Officer is able to act independently and report directly to the senior management or to the Board of Directors. Principal Officer shall be located at the head/corporate office of the bank and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. He will maintain close liaison with enforcement agencies, banks and any other institution which are involved in the fight against money laundering and combating financing of terrorism

Further, the role and responsibilities of the Principal Officer should include overseeing and ensuring overall compliance with regulatory guidelines on KYC/AML/CFT issued from time to time and obligations under the Prevention of Money Laundering Act, 2002, rules and regulations made thereunder, as amended form time to time. The Principal Officer will also be responsible for timely submission of CTR, STR and reporting of counterfeit notes and all transactions involving receipts by non-profit organisations of value more than Rupees Ten Lakh or its

equivalent in foreign currency to FIU-IND.With a view to enabling the Principal Officer to discharge his responsibilities effectively, the Principal Officer and other appropriate staff should have timely access to customer identification data and other CDD information, transaction records and other relevant information.

2.24. Maintenance of records of transactions/Information to be preserved/Maintenance and preservation of records/Cash and Suspicious transactions reporting to Financial Intelligence Unit- India (FIU-IND)

Section 12 of the PMLA, 2002 casts certain obligations on the banking companies in regard to preservation and reporting of customer account information. Banks are, therefore, advised to go through the provisions of PMLA, 2002 and the Rules notified there under and take all steps considered necessary to ensure compliance with the requirements of Section 12 of the Act *ibid.*

a) Maintenance of records of transactions

Banks should introduce a system of maintaining proper record of transactions prescribed under Rule 3 of PML Rules, 2005, as mentioned below:

i) All cash transactions of the value of more than Rupees Ten Lakh or its equivalent in foreign currency;

ii)All series of cash transactions integrally connected to each other which have been valued below Rupees Ten Lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds Rupees Ten Lakh;

Explanation - Integrally connected cash transactions referred to at (ii) above

The following transactions have taken place in a branch during the month of April 2008:

Date	Mode	Dr (in Rs.)	Cr (in Rs.)	Balance (in Rs.) BF - 8,00,000.00
02/04/2008	Cash	5,00,000.00	3,00,000.00	6,00,000.00
07/04/2008	Cash	40,000.00	2,00,000.00	7,60,000.00
08/04/2008	Cash	4,70,000.00	1,00,000.00	3,90,000.00
Monthly summation		**10,10,000.00**	**6,00,000.00**	

63

iii) As per above clarification, the debit transactions in the above example are integrally connected cash transactions because total cash debits during the calendar month exceeds Rs. 10 lakhs

iv) All transactions involving receipts by non-profit organisations of value more than rupees ten lakh or its equivalent in foreign currency [Ref: Government of India Notification dated November 12, 2009- Rule 3,sub-rule (1) clause (BA) of PML Rules]

v) All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security or a document has taken place facilitating the transaction and

vi) All suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.

vii) All the credit transactions in the above example would not be treated as integrally connected, as the sum total of the credit transactions during the month does not exceed Rs.10 lakh and hence credit transaction dated 02, 07 & 08/04/2008 should not be reported by banks.

b) Information to be preserved

Banks are required to maintain all necessary information in respect of transactions referred to in PML Rule 3 to permit reconstruction of individual transaction, including the following information:

i) the nature of the transactions;

ii) the amount of the transaction and the currency in which it was denominated;

iii) the date on which the transaction was conducted; and

iv) the parties to the transaction.

c) Maintenance and Preservation of Records

i) Banks are required to maintain the records containing information of all transactions including the records of transactions detailed in Rule 3 above. Banks should take appropriate steps to evolve a system for proper maintenance and preservation of account information in a

manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities. Further, in terms of PML Amemdment Act 2012 notified on February 15, 2013, banks should maintain for at least five years from the date of transaction between the bank and the client, all necessary records of transactions, both domestic or international, which will permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.

ii) Banks should ensure that records pertaining to the identification of the customer and his address (e.g. copies of documents like passports, identity cards, driving licenses, PAN card, utility bills etc.) obtained while opening the account and during the course of business relationship, are properly preserved for at least five years **after the business relationship is ended** as required under Rule 10 of the Rules *ibid*. The identification records and transaction data should be made available to the competent authorities upon request.

iii) In paragraph 2.13 of this Master Circular, banks have been advised to pay special attention to all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. It is further clarified that the background including all documents/office records/memorandums pertaining to such transactions and purpose thereof should, as far as possible, be examined and the findings at branch as well as Principal Officer level should be properly recorded. Such records and related documents should be made available to help auditors in their day-to-day work relating to scrutiny of transactions and also to Reserve Bank/other relevant authorities. These records are required to be preserved for ten years as is required under PMLA, 2002.

d) Reporting to Financial Intelligence Unit - India

i) In terms of the PMLA Rules, banks are required to report information

65

relating to cash and suspicious transactions and all transactions involving receipts by non-profit organisations of value more than rupees ten lakh or its equivalent in foreign currency to the Director, Financial Intelligence Unit-India (FIU-IND) in respect of transactions referred to in Rule 3 at the following address:

Director, FIU-IND,
Financial Intelligence Unit-India,
6th Floor, Hotel Samrat,
Chanakyapuri,
New Delhi -110021
Website - http://fiuindia.gov.in/

Explanation: Government of India Notification dated November 12, 2009- Rule 2 sub-rule (1) clause (ca) defines Non-Profit Organization (NPO). NPO means any entity or organisation that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under section 25 of the Companies Act, 1956.

ii) The earlier prescribed multiple data files reporting format has been replaced by a new single XML file format. FIU-IND has released a comprehensive reporting format guide to describe the specifications of prescribed reports to FIU-IND. FIU-IND has also developed a Report Generation Utility and Report Validation Utility to assist reporting entities in the preparation of prescribed reports. The OM issued on Reporting Formats under Project FINnet dated 31st March,2011 by FIU containing all relevant details are available on FIU's website. Banks In this regard, a reference is also invited to circualrs DBOD.AML.BC.No.39/14.01.001/2012-13 and DBOD.AML.BC.No.49/14.01.001/2012-13 dated September 7, 2012 and October 11, 2012 respectively. Accordingly, banks should carefully go through all the reporting formats prescribed by FIU-IND. Accordingly, banks should carefully go through all the reporting formats prescribed by FIU-IND.

iii) FIU-IND have placed on their website editable electronic utilities to

66

enable banks to file electronic CTR/STR who are yet to install/adopt suitable technological tools for extracting CTR/STR from their live transaction data base. It is, therefore, advised that in cases of banks, where all the branches are not fully computerized, the Principal Officer of the bank should cull out the transaction details from branches which are not yet computerized and suitably arrange to feed the data into an electronic file with the help of the editable electronic utilities of CTR/STR as have been made available by FIU-IND on their website http://fiuindia.gov.in

In terms of instructions contained in paragraph 2.3(b) of this Master Circular, banks are required to prepare a profile for each customer based on risk categorisation. Further, vide paragraph 2.13(d), the need for periodical review of risk categorisation has been emphasized. It is, therefore, reiterated that banks, as a part of transaction monitoring mechanism, are required to put in place an appropriate software application to throw alerts when the transactions are inconsistent with risk categorization and updated profile of customers. It is needless to add that a robust software throwing alerts is essential for effective identification and reporting of suspicious transaction.

2.25. Various Reporting Formats

a) **Cash Transaction Report (CTR)**

While detailed instructions for filing all types of reports are given in the instructions part of the related formats, banks should scrupulously adhere to the following:

i) The Cash Transaction Report (CTR) for each month should be submitted to FIU-IND by 15th of the succeeding month. Cash transaction reporting by branches to their controlling offices should, therefore, invariably be submitted on monthly basis (not on fortnightly basis) and banks should ensure to submit CTR for every month to FIU-IND within the prescribed time schedule.

67

ii) All cash transactions, where forged or counterfeit Indian currency notes have been used as genuine should be reported by the Principal Officer to FIU-IND in the specified format not later than seven working days from the date of occurrence of such transactions (Counterfeit Currency Report – CCR). These cash transactions should also include transactions where forgery of valuable security or documents has taken place and may be reported to FIU-IND in plain text form.

iii) While filing CTR, details of individual transactions below Rupees Fifty thousand need not be furnished.

iv) CTR should contain only the transactions carried out by the bank on behalf of their clients/customers excluding transactions between the internal accounts of the bank.

v) A summary of cash transaction report for the bank as a whole should be compiled by the Principal Officer of the bank every month in physical form as per the format specified. The summary should be signed by the Principal Officer and submitted to FIU-India.

vi) In case of Cash Transaction Reports (CTR) compiled centrally by banks for the branches having Core Banking Solution (CBS) at their central data centre level, banks may generate centralised Cash Transaction Reports (CTR) in respect of branches under core banking solution at one point for onward transmission to FIU-IND, provided:

a) The CTR is to be generated in the format prescribed by FIU-IND;

b) A copy of the monthly CTR submitted on its behalf to FIU-India is available at the concerned branch for production to auditors/inspectors, when asked for; and

68

c) The instruction on 'Maintenance of records of transactions'; 'Information to be preserved' and 'Maintenance and Preservation of records' as contained above in this Master Circular at Para 2.24 (a), (b) and (c) respectively are scrupulously followed by the branch.

However, in respect of branches not under CBS, the monthly CTR should continue to be compiled and forwarded by the branch to the Principal Officer for onward transmission to FIU-IND.

b) **Suspicious Transaction Reports (STR)**

i) While determining suspicious transactions, banks should be guided by definition of suspicious transaction contained in PMLA Rules as amended from time to time.

ii) It is likely that in some cases transactions are abandoned/aborted by customers on being asked to give some details or to provide documents. It is clarified that banks should report all such attempted transactions in STRs, even if not completed by customers, irrespective of the amount of the transaction.

iii) Banks should make STRs if they have reasonable ground to believe that the transaction involve proceeds of crime generally irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences in part B of Schedule of PMLA, 2002.

iv) The STR should be furnished within seven days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer should record his reasons for treating any transaction or a series of transactions as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion once a suspicious transaction

report is received from a branch or any other office. Such report should be made available to the competent authorities on request.

v) In the context of creating KYC/AML awareness among the staff and for generating alerts for suspicious transactions, banks may consider the indicative list of suspicious activities contained in Annex-E of the 'IBA's Guidance Note for Banks, January 2012'.

vi) Banks should not put any restrictions on operations in the accounts where an STR has been made. Banks and their employees should keep the fact of furnishing of STR strictly confidential, as required under PML Rules. It should be ensured that there is no tipping off to the customer at any level.

c) **Non-Profit Organisation**

The report of all transactions involving receipts by non- profit organizations of value more than rupees ten lakh or its equivalent in foreign currency should be submitted every month to the Director, FIU-IND by 15th of the succeeding month in the prescribed format.

d) **Cross-border Wire Transfer**

Cross-border Wire Transfer Report (CWTR) is required to be filed by 15th of succeeding month for all cross border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency where either the origin or destination of fund is in India.

2.26. Customer Education/Employee's Training/Employee's Hiring

a) **Customer Education**

Implementation of KYC procedures requires banks to demand certain information from customers which may be of personal nature or which has hitherto never been called for. This can sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information. There is, therefore, a need for banks to prepare specific literature/ pamphlets etc. so as to educate the customer of the objectives of the KYC programme. The front desk staff needs to be specially trained to handle such situations while dealing with customers.

70

b) **Employees' Training**

Banks must have an ongoing employee training programme so that the members of the staff are adequately trained in KYC procedures. Training requirements should have different focuses for frontline staff, compliance staff and staff dealing with new customers. It is crucial that all those concerned fully understand the rationale behind the KYC policies and implement them consistently.

c) **Hiring of Employees**

It may be appreciated that KYC norms/AML standards/CFT measures have been prescribed to ensure that criminals are not allowed to misuse the banking channels. It would, therefore, be necessary that adequate screening mechanism is put in place by banks as an integral part of their recruitment/hiring process of personnel.

Annex- I

Customer Identification Procedure

Documents that may be obtained from customers

Features	Documents
Accounts of individuals	
- Proof of Identity	(i) Passport (ii) PAN card (iii) Voter's Identity Card (iv) Driving License (v)Job Card issued by NREGA duly signed by an officer of the State Govt (vi) The letter issued by the Unique Identification Authority of India (UIDAI) containing details of name, address and Aadhaar number (vii) Identity card (subject to the bank's satisfaction) (viii) Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of bank
- Proof of Address	Any one of the documents from the above submitted as proof of identity which contains an address or any of the following:

71

	(i) Telephone bill (ii) Bank account statement (iii) Letter from any recognized public authority (iv) Electricity bill (v) Ration card (vi) Letter from employer (subject to satisfaction of the bank) ((vii) A rent agreement indicating the address of the customer duly registered with State Government or similar registration authority.
Accounts of companies - Name of the company - Principal place of business - Mailing address of the company - Telephone/Fax Number	(i) Certificate of incorporation and Memorandum & Articles of Association (ii) Resolution of the Board of Directors to open an account and identification of those who have authority to operate the account (iii) Power of Attorney granted to its managers, officers or employees to transact business on its behalf (iv) Copy of PAN allotment letter (v) Copy of the telephone bill
Accounts of partnership firms - Legal name - Address - Names of all partners and their addresses - Telephone numbers of the firm and partners	(i) Registration certificate, if registered (ii) Partnership deed (iii) Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf (iv) Any officially valid document identifying the partners and the persons holding the Power of Attorney and their addresses (v) Telephone bill in the name of firm/partners
Accounts of trusts & foundations - Names of trustees, settlors, beneficiaries and signatories - Names and addresses of the founder, the managers/directors and the beneficiaries - Telephone/fax numbers	(i) Certificate of registration, if registered (ii) Power of Attorney granted to transact business on its behalf (iii) Any officially valid document to identify the trustees, settlors, beneficiaries and those holding Power of Attorney, founders/managers/ directors and their addresses (iv) Resolution of the managing body of the foundation/association (v) Telephone bill

72

Accounts of Proprietorship Concerns Proof of the name, address and activity of the concern	• Registration certificate (in the case of a registered concern) • Certificate/licence issued by the Municipal authorities under Shop & Establishment Act, • Sales and income tax returns • CST/VAT certificate • Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities • Licence issued by the Registering authority like Certificate of Practice issued by Institute of Chartered Accountants of India, Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food and Drug Control Authorities, registration/licensing document issued in the name of the proprietary concern by the Central Government or State Government Authority/ Department, etc. Banks may also accept IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT as an identity document for opening of the bank account etc. • The complete Income Tax return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/ acknowledged by the Income Tax Authorities. • Utility bills such as electricity, water, and landline telephone

	bills in the name of the proprietary concern. Any two of the above documents would suffice. These documents should be in the name of the proprietary concern.

Annex -II

File No.17015/10/2002-IS-VI
Government of India
Ministry of Home Affairs
Internal Security-I Division

New Delhi, dated 27th August, 2009

ORDER

Subject : Procedure for implementation of Section 51A of the Unlawful Activities (Prevention)Act, 1967

The Unlawful Activities (Prevention) Act, 1967 (UAPA) has been amended and notified on 31.12.2008, which, inter-alia, inserted Section 51A to the Act. Section 51A reads as under:-

"51A. For the prevention of, and for coping with terrorist activities, the Central Government shall have power to –

(a) freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of or at the direction of the individuals or entities Listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism;

(b) prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals

74

or entities Listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism;

(c) prevent the entry into or the transit through India of individuals Listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism",

The Unlawful Activities (Prevention) Act define "Order" as under:-

"Order" means the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as may be amended from time to time.

In order to expeditiously and effectively implement the provisions of Section 51A, the following procedures shall be followed:-

Appointment and Communication of details of UAPA nodal officers

2. As regards appointment and communication of details of UAPA nodal officers -

(i) The UAPA nodal officer for IS-I division would be the Joint Secretary (IS.I), Ministry of Home Affairs. His contact details are 011-23092736(Tel), 011-23092569(Fax) and isis@nic.in (e-mail ID).

(ii) The Ministry of External Affairs, Department of Economic Affairs, Foreigners Division of MHA, FIU-IND; and RBI, SEBI, IRDA (hereinafter referred to as Regulators) shall appoint a UAPA nodal officer and communicate the name and contact details to the IS-I Division in MHA.

(iii) The States and UTs should appoint a UAPA nodal officer preferably of the rank of the Principal Secretary/Secretary, Home Department and communicate the name and contact details to the IS-I Division in MHA.

(iv) The IS-I Division in MHA would maintain the consolidated list of all UAPA nodal officers and forward the list to all other UAPA nodal officers.

(v) The RBI, SEBI, IRDA should forward the consolidated list of UAPA nodal officers to the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies respectively.

(vi) The consolidated list of the UAPA nodal officers should be circulated to the nodal officer of IS-I Division of MHA in July every year and on every change. Joint Secretary(IS-I), being the nodal officer of IS-I Division of MHA, shall cause the amended list of UAPA nodal officers to be circulated to the nodal officers of Ministry of External Affairs, Department of Economic Affairs, Foreigners Division of MHA, RBI, SEBI, IRDA and FIU-IND.

75

Communication of the list of designated individuals/entities

3. As regards communication of the list of designated individuals/entities-

(i) The Ministry of External Affairs shall update the list of individuals and entities subject to UN sanction measures on a regular basis. On any revision, the Ministry of External Affairs would electronically forward this list to the Nodal Officers in Regulators, FIU-IND, IS-I Division and Foreigners' Division in MHA.

(ii) The Regulators would forward the list mentioned in (i) above (referred to as designated lists) to the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies respectively.

(iii) The IS-I Division of MHA would forward the designated lists to the UAPA nodal officer of all States and UTs.

(iv) The Foreigners Division of MHA would forward the designated lists to the immigration authorities and security agencies.

Regarding funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or insurance policies etc.

4. As regards funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or insurance policies etc., the Regulators would forward the designated lists to the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies respectively. The RBI, SEBI and IRDA would issue necessary guidelines to banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies requiring them to -

(i) Maintain updated designated lists in electronic form and run a check on the given parameters on a regular basis to verify whether individuals or entities listed in the schedule to the Order (referred to as designated individuals/entities) are holding any funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or insurance policies etc. with them.

(ii) In case, the particulars of any of their customers match with the particulars of designated individuals/entities, the banks, stock exchanges/ depositories, intermediaries regulated by SEBI and insurance companies shall immediately, not later than 24 hours from the time of finding out such customer, inform full particulars of the funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or insurance policies etc. held by such customer on their books to the Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No.011-23092569 and

76

also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on e-mail id: jsis@nic.in.

(iii) The banks, stock exchanges/ depositories, intermediaries regulated by SEBI and insurance companies shall also send by post a copy of the communication mentioned in (ii) above to the UAPA nodal officer of the state/ UT where the account is held and Regulators and FIU-IND, as the case may be.

(iv) In case, the match of any of the customers with the particulars of designated individuals/entities is beyond doubt, the banks stock exchanges / depositories, intermediaries regulated by SEBI and insurance companies would prevent designated persons from conducting financial transactions, under intimation to Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No. 011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on e-mail id: jsis@nic.in.

(v) The banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies shall file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions in the accounts covered by paragraph (ii) above , carried through or attempted, as per the prescribed format.

5. On receipt of the particulars referred to in paragraph 3(ii) above, IS-I Division of MHA would cause a verification to be conducted by the State Police and/or the Central Agencies so as to ensure that the individuals/entities identified by the banks, stock exchanges/depositories, intermediaries regulated by SEBI and Insurance Companies are the ones listed as designated individuals/entities and the funds, financial assets or economic resources or related services, reported by banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies are held by the designated individuals/entities. This verification would be completed within a period not exceeding 5 working days from the date of receipt of such particulars.

6. In case, the results of the verification indicate that the properties are owned by or held for the benefit of the designated individuals/entities, an order to freeze these assets under section 51A of the UAPA would be issued within 24 hours of such verification and conveyed electronically to the concerned bank branch, depository, branch of insurance company branch under intimation to respective Regulators and FIU-IND. The UAPA nodal officer of IS-I Division of MHA shall also forward a copy thereof to all the Principal Secretary/Secretary, Home Department of the States or UTs, so that any individual or entity may be prohibited from making any funds, financial assets or economic assets or economic resources or related services available for the benefit of the designated individuals/entities or any other person engaged in or suspected to be engaged

77

in terrorism. The UAPA nodal officer of IS-I Division of MHA shall also forward a copy of the order under Section 51A, to all Directors General of Police/Commissioners of Police of all states/UTs for initiating action under the provisions of Unlawful Activities (Prevention) Act.

The order shall take place without prior notice to the designated individuals/entities.

Regarding financial assets or economic resources of the nature of immovable properties.

7. IS-I Division of MHA would electronically forward the designated lists to the UAPA nodal officer of all States and UTs with the request to have the names of the designated individuals/entities, on the given parameters, verified from the records of the office of the Registrar performing the work of registration of immovable properties in their respective jurisdiction.

8. In case, the designated individuals/entities are holding financial assets or economic resources of the nature of immovable property and if any match with the designated individuals/entities is found, the UAPA nodal officer of the State/UT would cause communication of the complete particulars of such individual/entity along with complete details of the financial assets or economic resources of the nature of immovable property to the Joint Secretary (IS.I), Ministry of Home Affairs, immediately within 24 hours at Fax No.011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on e-mail id: **jsis@nic.in**

9. The UAPA nodal officer of the State/UT may cause such inquiry to be conducted by the State Police so as to ensure that the particulars sent by the Registrar performing the work of registering immovable properties are indeed of these designated individuals/entities. This verification would be completed within a maximum of 5 working days and should be conveyed within 24 hours of the verification, if it matches with the particulars of the designated individual/entity to Joint Secretary(IS-I), Ministry of Home Affairs at the Fax telephone numbers and also on the e-mail id given below.

10. A copy of this reference should be sent to the Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No.011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post would necessarily be conveyed on e-mail id: **jsis@nic.in.** MHA may have the verification also conducted by the Central Agencies. This verification would be completed within a maximum of 5 working days.

11. In case, the results of the verification indicate that the particulars match with those of designated individuals/entities, an order under Section 51A of the

78

UAPA would be issued within 24 hours, by the nodal officer of IS-I Division of MHA and conveyed to the concerned Registrar performing the work of registering immovable properties and to FIU-IND under intimation to the concerned UAPA nodal officer of the State/UT.

The order shall take place without prior notice, to the designated individuals/entities.

12. Further, the UAPA nodal officer of the State/UT shall cause to monitor the transactions/accounts of the designated individual/entity so as to prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities listed in the schedule to the order or any other person engaged in or suspected to be engaged in terrorism. The UAPA nodal officer of the State/UT shall upon coming to his notice, transactions and attempts by third party immediately bring to the notice of the DGP/Commissioner of Police of the State/UT for also initiating action under the provisions of Unlawful Activities (Prevention) Act.

Implementation of requests received from foreign countries under U.N. Security Council Resolution 1373 of 2001.

13. U.N. Security Council Resolution 1373 obligates countries to freeze without delay the funds or other assets of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds or other assets derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons and entities. Each individual country has the authority to designate the persons and entities that should have their funds or other assets frozen. Additionally, to ensure that effective cooperation is developed among countries, countries should examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other countries.

14. To give effect to the requests of foreign countries under U.N. Security Council Resolution 1373, the Ministry of External Affairs shall examine the requests made by the foreign countries and forward it electronically, with their comments, to the UAPA nodal officer for IS-I Division for freezing of funds or other assets.

15. The UAPA nodal officer of IS-I Division of MHA, shall cause the request to be examined, within 5 working days so as to satisfy itself that on the basis of applicable legal principles, the requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances terrorism or a terrorist organization, and upon his satisfaction, request would be electronically forwarded to the nodal officers in Regulators. FIU-IND and to the nodal officers of

the States/UTs. The proposed designee, as mentioned above would be treated as designated individuals/entities.

16. Upon receipt of the requests by these nodal officers from the UAPA nodal officer of IS-I Division, the procedure as enumerated at paragraphs 4 to 12 above shall be followed.

The freezing orders shall take place without prior notice to the designated persons involved.

Procedure for unfreezing of funds, financial assets or economic resources or related services of individuals/entities inadvertently affected by the freezing mechanism upon verification that the person or entity is not a designated person

17. Any individual or entity, if it has evidence to prove that the freezing of funds, financial assets or economic resources or related services, owned/held by them has been inadvertently frozen, they shall move an application giving the requisite evidence, in writing, to the concerned bank, stock exchanges/depositories, intermediaries regulated by SEBI, insurance companies, Registrar of Immovable Properties and the State/UT nodal officers.

18. The banks stock exchanges/depositories, intermediaries regulated by SEBI, insurance companies, Registrar of Immovable Properties and the State/UT nodal officers shall inform and forward a copy of the application together with full details of the asset frozen given by any individual or entity informing of the funds, financial assets or economic resources or related services have been frozen inadvertently, to the nodal officer of IS-I Division of MHA as per the contact details given in paragraph 4(ii) above within two working days.

19. The Joint Secretary (IS-I), MHA, being the nodal officer for (IS-I) Division of MHA, shall cause such verification as may be required on the basis of the evidence furnished by the individual/entity and if he is satisfied, he shall pass an order, within 15 working days, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant under intimation to the concerned bank, stock exchanges/depositories, intermediaries regulated by SEBI, insurance company and the nodal officers of States/UTs. However, if it is not possible for any reason to pass an order unfreezing the assets within fifteen working days, the nodal officer of IS-I Division shall inform the applicant.

Communication of Orders under section 51A of Unlawful Activities (Prevention) Act.

20. All Orders under section 51A of Unlawful Activities (Prevention) Act, relating to funds, financial assets or economic resources or related services, would be communicated to all banks, depositories/stock exchanges,

80

intermediaries regulated by SEBI, insurance companies through respective Regulators, and to all the Registrars performing the work of registering immovable properties, through the State/UT nodal officer by IS-I Division of MHA.

Regarding prevention of entry into or transit through India

21. As regards prevention of entry into or transit through India of the designated individuals, the Foreigners Division of MHA, shall forward the designated lists to the immigration authorities and security agencies with a request to prevent the entry into or the transit through India. The order shall take place without prior notice to the designated individuals/entities.

22. The immigration authorities shall ensure strict compliance of the Orders and also communicate the details of entry or transit through India of the designated individuals as prevented by them to the Foreigners' Division of MHA.

Procedure for communication of compliance of action taken under Section 51A.

23. The nodal officers of IS-I Division and Foreigners Division of MHA shall furnish the details of funds, financial assets or economic resources or related services of designated individuals/entities frozen by an order, and details of the individuals whose entry into India or transit through India was prevented, respectively, to the Ministry of External Affairs for onward communication to the United Nations.

24. All concerned are requested to ensure strict compliance of this order.

(D .Diptivilasa)
Joint Secretary to Government of India

81

Annex - III

Government of India
Ministry of Finance
(Department of Revenue)

Notification

New Delhi, the 16th December 2010

GSR ------ (E) – In exercise of the powers conferred by sub-section (1) read with clauses (h) (i), (j) and (k) of sub-section (2) of Section 73 of the Prevention of Money-laundering Act, 2002 (15 of 2003), the Central Government hereby makes the following amendments to the Prevention of Money-laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005, namely::-

1. (1) These rules may be called the Prevention of Money-laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Third Amendment Rules, 2010.

(2) They shall come into force on the date of their publication in the Official Gazette.

82

2. In the Prevention of Money-laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005, -

(a) in rule 2,-

(i) after clause (b), the following clause shall be inserted, namely:-

"(bb) "Designated Officer" means any officer or a class of officers authorized by a banking company, either by name or by designation, for the purpose of opening small accounts".

(ii) in clause (d), for the words "the Election Commission of India or any other document as may be required by the banking company or financial institution or intermediary", the words "Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government, the letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number or any other document as notified by the Central Government in consultation with the Reserve Bank of India or any other document as may be required by the banking companies, or financial institution or intermediary" shall be substituted;

(iii) after clause (fa), the following clause shall be inserted, namely:-

"(fb) "small account" means a savings account in a banking company where-

(i) the aggregate of all credits in a financial year does not exceed rupees one lakh,
(ii) the aggregate of all withdrawals and transfers in a month does not exceed rupees ten thousand, and;
(iii) the balance at any point of time does not exceed rupees fifty thousand".

(b) In rule 9, after sub-rule (2), the following sub-rule shall be inserted, namely:-

"(2A) Notwithstanding anything contained in sub-rule (2), an individual who desires to open a small account in a banking company may be allowed to open such an account on production of a self-attested photograph and affixation of signature or thumb print, as the case may be, on the form for opening the account.

Provided that –

(i) the designated officer of the banking company, while opening the small account, certifies under his signature that the person opening the account has affixed his signature or thumb print, as the case may be, in his presence;

(ii) a small account shall be opened only at Core Banking Solution linked banking company branches or in a branch where it is possible to manually monitor and ensure that foreign remittances are not credited to a small account and that the stipulated limits on monthly and annual aggregate of transactions and balance in such accounts are not breached, before a transaction is allowed to take place;

(iii) a small account shall remain operational initially for a period of twelve months, and thereafter for a further period of twelve months if the holder of such an account provides evidence before the banking company of having applied for any of the officially valid documents within twelve months of the opening of the said account, with the entire relaxation provisions to be reviewed in respect of the said account after twenty four months.

(iv) a small account shall be monitored and when there is suspicion of money laundering or financing of terrorism or other high risk scenarios, the identity of client shall be established through the production of officially valid documents, as referred to in sub rule (2) of rule 9"; and

(v) foreign remittance shall not be allowed to be credited into a small account unless the identity of the client is fully established through the production of officially valid documents, as referred to in sub-rule (2) of rule 9."

(Notification No.14/2010/F.No.6/2/2007-ES)

(S.R. Meena)
Under Secretary

Note: The principal rules were published in Gazette of India, Extraordinary, Part-II, Section 3, Sib-Section (i) vide number G.S.R.444 (E), dated the 1st July, 2005 and subsequently amended by number G.S.R.717 (E), dated the 13th December, 2005, number G.S.R. 389(E), dated the 24th May, 2007, number G.S.R. 816(E), dated the 12th November, 2009, number G.S.R.76 (E), dated the 12th February, 2010 and number G.S.R. 508(E), dated the 16th June, 2010.

84

ANNEX –IV

(List of Circulars on 'Know Your Customer' and monitoring of transactions consolidated in the Master Circular)

Sr. No.	Circular No. and date	Subject	Gist of instructions
1	DBOD.BP.BC.92/C.469-76 dated 12th August, 1976	Issue of DDs/TTs in excess of Rs.5000/-	Applicants (whether customer or not) for DD/MT/TT/Travellers cheques for amount exceeding Rs.10,000/- should affix Permanent Income Tax Number on the application.
2	DBOD.GC.BC.62/c.408(A)/87 dated 11th November, 1987	Frauds in banks-opening of new accounts.	Payment for imports should be made by debit to the accounts maintained with the same bank or any other bank and under no circumstances cash should be accepted for retirement of import bills. There should be reasonable gap of say, 6 months between the time an introducer opens his account and introduces another prospective account holder to the bank. Introduction of an account should enable proper identification of the person opening an account so that the person can be traced if the account is misused.
3	DBOD.BP.BC.114/C.469 (81)-91 dated 19th April, 1991	Misuse of banking channels for violation of fiscal laws and evasion of taxes – Issue and payment of demand drafts for Rs.50,000 and above.	Banks to issue travellers cheques, demand drafts, mail transfers, telegraphic transfers for Rs. 50,000/- and above by debit to customers accounts or against cheques only and not against cash.
4	DBOD.BC.20/17.04.001/92 dated 25th August, 1992	Committee to enquire into various aspects relating to frauds	Banks advised to adhere to the prescribed norms and safeguards while opening accounts etc.

85

Sr. No.	Circular No. and date	Subject	Gist of instructions
		and malpractices in banks.	
5	DBOD.BP.BC.60/21.01.023/92 dated 21st December,1992	Diversion of working capital funds.	Banks to ensure that withdrawals from cash credit/overdraft accounts are strictly for the purpose for which the credit limits were sanctioned by them. There should be no diversion of working capital finance for acquisition of fixed assets, investments in associate companies/ subsidiaries and acquisition of shares, debentures, units of UTI and other mutual funds and other investments in the capital market.
6	DBOD.FMC.No. 153/27.01.003/93-94 dated 1st September, 1993	Monitoring of flow of funds.	Banks to be vigilant and ensure proper end use of bank funds/monitoring flow of funds. Banks to keep vigil over heavy cash withdrawals by account holders which may be disproportionate to their normal trade/business requirements and cases of unusual trends. Doubtful cases to be reported to DBOD, Regional office.
7	DBOD.GC.BC.193/17.04.001/93 dated 18th November, 1993	Frauds in banks – Encashment of Interest/Dividend Warrants, Refund Orders etc.	Banks to be vigilant in opening new accounts without proper introduction, new accounts with fictitious names and addresses. Banks instructed to strictly adhere to the instructions issued on opening and operating of bank accounts.
8	DBOD.GC.BC.202/17.04.001/93 dated 6th December, 1993	The Committee to enquire into various aspects relating to frauds and malpractices in banks.	Customer identification while opening accounts including obtaining of photographs of customers while opening accounts.
9	DBOD.No.GC.BC.46/17.04.001 dated 22nd April,	The Committee to enquire into various aspects	Clarifications given to banks regarding obtaining photographs of the depositors/account holder

86

Sr. No.	Circular No. and date	Subject	Gist of instructions
	1994	relating to frauds and malpractices in banks.	authorised to operate new accounts with effect from 1.1.1994. Obtaining of photographs would apply to residents and non-residents and all categories of deposits including fixed/recurring/cumulative deposit accounts and also to those persons authorised to operate the accounts.
10	DBOD.BP.BC.106/21.01.001/94 dated 23rd September,1994	Fraudulent operations in deposit accounts-opening and collection of cheques/pay orders etc.	Banks to examine every request for opening joint accounts very carefully, look into the purpose, other relevant aspects relating to business, the financial position of the account holders and whether number of account holders are large. 'Generally crossed' cheques and payable to 'order' should be collected only on proper endorsement by the payee. Banks to exercise care in collection of cheques of large amounts and ensure that joint accounts are not used for benami transactions.
11	DBOD.BP.BC.57/21.01.001/95 dated 4th May, 1995	Frauds in banks – Monitoring of deposit accounts.	Banks to introduce system of close watch of new deposit accounts and monitoring of cash withdrawals and deposits for Rs.10 lakh and above in deposit, cash credit and overdraft accounts. Banks to keep record of details of these large cash transactions in a separate register.
12	DBOD.BP.BC.102/21.01.001/95 dated 20th September, 1995	Monitoring of Deposit Accounts.	Reporting of all cash deposits and withdrawals of Rs.10 lakhs and above with full details in fortnightly statements by bank branches to their controlling offices. Transactions of suspicious nature

87

Sr. No.	Circular No. and date	Subject	Gist of instructions
			to be apprised to Head Office. RBI to look into these statements at the time of inspections
13	DBOD.BP.BC.42/21.01.001/96 dated 6th April, 1996	Monitoring cash deposits and withdrawals of Rs.10 lakh and above in deposit/other accounts.	Banks asked to submit feedback on implementation of the system of close monitoring of large cash deposits and withdrawals of Rs.10 lakh and above.
14	DBOD.No.BP.BC.12/21.01.023/98 dated 11th February 1998	Furnishing of data-violation of secrecy obligations.	Banks should satisfy themselves that information sought will not violate the laws relating to secrecy in banking transactions except under compulsion of law, duty to the public to disclose, where interest of bank requires disclosure and where disclosure is made with the express or implied consent of the customer.
15	DBS.FGV.BC.56.23.04.001/98-99 dated 21st June, 1999	Report of the Study Group on Large Value Bank Frauds.	Banks advised to implement the main recommendations of the Study Group on Large Value Bank Frauds.
16	DBOD.COMP.BC.No.130/07.03.23/2000-01 dated 14th June, 2001	Internet Banking in India-Guidelines.	Banking facilities on Internet will be subject to the existing regulatory framework. Banks having physical presence in India only will be allowed to offer banking services over Internet to residents in India and any cross border transactions will be subject to existing exchange control regulations. Banks to establish identity and also make enquiries about integrity and reputation of the prospective customer. Internet accounts should be opened only after proper introduction and physical verification of the identity of the customer.
17	DBOD.BP.52/21.01.001/2001-02	Prevention of Terrorism	Banks should keep a watchful eye on the transactions of the 23

Sr. No.	Circular No. and date	Subject	Gist of instructions
	dated 5th December, 2001	Ordinance,2001-Implementation thereof.	terrorist organisations listed in the Schedule to the Ordinance. Violations of the extant Acts or normal banking operations must be reported to the appropriate authorities under the Ordinance under advice to RBI. Banks to undertake 'due diligence' in respect of the 'KYC' principle.
18	DBOD.AML.BC. 89/14.01.001/2001-02 dated 15th April, 2002	Freezing of funds pursuant to United Nations Security Council Resolution, 1390.	Accounts of individuals and entities listed should be immediately frozen as informed by the Security Council Sanctions Committee of the UN. If any transaction is detected involving any of these entities, banks to report to RBI promptly for necessary action.
19	DBOD.AML.BC. No.102/14.01.001/2001-02 dated 10th May,2002	Monitoring of accounts - compliance with instructions.	Banks should ensure that no new accounts are opened by banned organisations. Banks to strictly adhere to the extant guidelines regarding opening and monitoring of accounts. Banks to confirm having issued instructions for immediate compliance by the branches and controlling offices.
20	DBOD.AML.BC. 18/14.01.001/2002-03 dated August 16, 2002	Guidelines on "Know Your Customer" norms and "Cash transactions"	First circular on KYC. The customer identification should entail verification through an introductory reference from an existing account holder/a person known to the bank or on the basis of documents provided by the customer. The Board of Directors of the banks should have in place adequate policies that establish procedures to verify the bonafide identification of individual/ corporates opening an account. Branches of banks are required to report all cash deposits and

89

Sr. No.	Circular No. and date	Subject	Gist of instructions
			withdrawals of Rs.10 lakhs and above as well as transactions of suspicious nature with full details in fortnightly statements to their controlling offices.
21	DBOD.NO.AML. BC.58/14.01.001 /2004-05 dated November 29, 2004	'Know Your Customer' (KYC) Guidelines – Anti Money Laundering Standards	Our guidelines were revisited to make those compliant with FATF recommendations and Basel Committee Report on CDD. Four pronged approach was prescribed to banks based on Customer Acceptance Policy, Customer Identification Procedure, Monitoring of Transaction and Risk Management.
22	DBOD.NO.AML. BC.28 /14.01.001/2005 -06 dated August 23, 2005	Know Your Customer Guidelines- Anti-Money Laundering Standards	KYC guidelines on document requirement were relaxed for people belonging to financially disadvantageous sections in the society, who could open account with introductory reference.
23	DBOD.NQ.AML. BC.63/14.01.001 /2005-06 dated February 15, 2006	Prevention of Money Laundering Act, 2002 – Obligation of banks in terms of Rules notified thereunder	Reporting mechanism and formats were prescribed to banks to report cash and suspicious transactions to Financial Intelligence Unit- India (FIU-IND).
24	DBOD.AML.BC. No.77/ 14.01.001 / 2006-07 April 13, 2007	Wire transfers	Banks were advised to ensure that all wire transfers involving domestic and cross border fund transfers are accompanied by full originator information.
25	DBOD.AML.BC. No. 63/ 14.01.001/2007-08 dated February 18, 2008	Know Your Customer (KYC) Norms/Anti Money Laundering (AML) Standards/Combating of Financing of Terrorism	Revised guidelines on KYC/AML issued on review of risk categorization of customers; periodical updation of customer identification data and screening mechanism for recruitment /hiring process of personnel.

90

Sr. No.	Circular No. and date	Subject	Gist of instructions
		(CFT)	
26	DBOD.AML.BC. No. 85/ 14.01.001/ 2007 -08 dated May 22, 2008	Prevention of Money Laundering Act, 2002 – Obligation of banks in terms of Rules notified thereunder.	Revised guidelines issued on CTR and STR by banks to FIU-IND.
27	DBOD.AML.BC. No.12/14.01.001 /2008-09 dated July 1, 2008	Master Circular – KYC norms/AML Standards/CFT/ Obligation of Banks under PMLA, 2002	The Master Circular consolidates all the guidelines issued by Reserve Bank of India on KYC/AML/CFT norms up to June 30, 2008
28	DBOD.AML.BC. No.2/14.01.001/ 2009-10 dated July 1, 2009	Master Circular – KYC norms/AML Standards/CFT/ Obligation of Banks under PMLA, 2002	The Master Circular consolidates all the guidelines issued by Reserve Bank of India on KYC/AML/CFT norms up to June 30, 2009
29	DBS.CO.FrMC. No. 2605/23.04.001/ 2009-10 dated August 18, 2009	Adherence to KYC/AML Guidelines while opening & conducting accounts of MLM Companies	Banks were advised to exercise caution when opening accounts of marketing and trading firms and to monitor cases when large number of cheque books were issued to such companies and small deposits in cash were being made in a/cs.
30	DBOD.AML.BC. No.43/14.01.001 /2009-10 dated September 11, 2009	KYC norms/AML standards/CFT/ Obligation of banks under PMLA, 2002	The Government amended the Prevention of Money Laundering Act, 2005 and it came into force with effect from June 01, 2009 as notified by the Government.
31	DBOD.AML.BC. No.44/14.01.001 /2009-10 dated September 17, 2009	Combating Financing of Terrorism-Unlawful Activities (Prevention) Act,(UAPA) 1967-Obligation of banks	Government of India, Ministry of Home Affairs issued an 'Order' dated August 27, 2009 detailing the procedure for implementation of Section 51A of UAPA
32	DBOD.AML.BC. No.68/14.01.001	Prevention of Money laundering	Government of India Notification dated November 12, 2009

91

Sr. No.	Circular No. and date	Subject	Gist of instructions
	/2009-10 dated January 12, 2009	(Amendment) Rules 2009- Obligation of banks /Financial Institutions	amended the Prevention of Money Laundering (Maintenance of records of the Intermediaries) Rules 2005
33	DBOD.AML.BC. No.80/14.01.001 /2009-10 dated March 26, 2010	Know Your Customer (KYC) guidelines- accounts of proprietary concerns	Customer identification procedure issued for account opening by proprietary concerns.
34	DBOD.AML.BC. No.95/14.01.001 /2009-10 dated April 23, 2010	Prevention of Money Laundering (Maintenance of records of the ...Intermediaries) Amendment Rules, 2010 - Obligation of banks	Government of India Notification dated February 12, 2010 amended the Prevention of Money Laundering (Maintenance of records of the Intermediaries) Rules 2005
35	DBOD.AML.BC. No.108/14.01.00 1/2009-10 dated June 9, 2010	KYC norms/AML standards/CFT/ Obligation of banks under PMLA, 2002	Further clarifications issued to banks in regard to: suspicion of money laundering or terrorist financing; filing of STRs; PEPs and Principal Officer.
36	DBOD.AML.BC. No.109/14.01.00 1/2009-10 dated June 10, 2010	KYC norms/AML standards/CFT/ Obligation of banks under PMLA, 2002	Guidelines reiterated for Client accounts opened by professional intermediaries
37	DBOD.AML.BC. No.111/14.01.00 1/2009-10 dated June 15, 2010	KYC norms/AML standards/CFT/ Obligation of banks under PMLA, 2002	Banks advised to take into account risks arising from deficiencies in AML/CFT regime of the Jurisdictions included in FATF Statement and also publicly available information of countries which do not or insufficiently apply the FATF recommendations and banks should not enter into relationship with shell banks.
38	DBOD.AML.BC. No.113/14.01.00	Prevention of Money	Government of India Notification dated June 16, 2010 amended the

92

Sr. No.	Circular No. and date	Subject	Gist of instructions
	1/2009-10 dated June 29, 2010	Laundering (Maintenance of records of the ...Intermediaries) Second Amendment Rules 2010	Prevention of Money Laundering (Maintenance of records of the Intermediaries) Rules 2005
39	DBOD.AML.BC. No.38/14.01.001 /2010-11 dated August 31, 2010	Accounts of proprietary concerns	An addition is made to the list of documents that may be accepted for opening a bank account in the name of a proprietary concern
40	DBOD.AML.BC. No.50/14.01.001 /2010-11 dated October 26, 2010	Opening of bank accounts - salaried employees	Banks need to rely on certification only from corporates and other entities of repute and should be aware of the competent authority designated by the concerned employer to issue such certificate/letter. In addition to the certificate from employer, banks should insist on at least one of the officially valid documents as provided in the PML Rules.
41	DBOD.AML.BC. No.65/14.01.001 /2010-11 dated December 7, 2010	Operation of bank accounts & money mules	Banks advised that operations of money mules can be minimized if banks follow the guidelines contained in the Master Circular on KYC/AML/CFT/obligations of banks under PMLA, 2002
42	DBOD.AML.BC. No.70/14.01.001 /2010-11 dated December 30, 2010	Accounts of bullion dealers (including sub-dealers) & jewelers should be categorized by banks as ' high risk'.	Accounts of bullion dealers (including sub-dealers) & jewelers should be categorized by banks as ' high risk'. requiring enhanced due diligence and intensified transaction monitoring. High risk associated with such accounts should also be taken into account to identify suspicious transactions for filing suspicious transaction reports (STRs) to FIU-IND.
43	DBOD.AML.BC. No.77/14.01.001 /2010-11 dated January 27,	Opening of "Small Account"	Government of India Notification dated December 16, 2011 amended the Prevention of Money Laundering (Maintenance of

93

Sr. No.	Circular No. and date	Subject	Gist of instructions
	2011		records of the Intermediaries) Rules 2005 to include definition of 'Small Account' and the detailed procedure for opening 'small accounts'.
44	DBOD.AML.BC. No.36/14.01.001 /2011-12 dated September 28, 2011.	Know Your Customer Norms – Letter issued by Unique Identification Authority of India (UIDAI) containing details of name, address and Aadhaar number	Letter issued by the UIDAI is accepted as an officially valid document for opening all types of bank accounts
45	DBOD.AML BC.No.47/14.01. 001/2011-12 dated November 04, 2011	Payment of Cheques/Drafts/ Pay Orders/ Banker's Cheques	With effect from April 1, 2012, cheques / Drafts/ Pay Orders/ Banker's cheques issued on or after April 1, 2012 are valid for three months from the date of issue.
46	DBOD. AML.BC. No.65 /14.01.001/2011 -12 dated December 19, 2011	Know Your Customer (KYC) norms/Anti-Money Laundering (AML) standards/Comba ting of Financing of Terrorism (CFT)/Obligation of banks under Prevention of Money Laundering Act (PMLA), 2002-Assessment and Monitoring of Risk	Banks may take steps to identify and assess their ML/TF risk for customers, countries and geographical areas as also for products/ services/ transactions/ delivery channels. Banks should also have policies, controls and procedures, duly approved by their boards, in place to effectively manage and mitigate their risk adopting a risk-based approach and adopt enhanced measures for products, services and customers with a medium or high risk rating.
47	DBOD AML BC No. 70	splitting of UNSC 1267	Banks may take into account both "Al-Qaida Sanctions List" and

94

Sr. No.	Circular No. and date	Subject	Gist of instructions
	/14.01.001/2011 -12 dated December 30, 2011	Committee's list of individuals and entities linked to Al-Qaida and Taliban	"1988 Sanctions List" for the purpose of implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967.
48	DBOD. AML.BC. No 93 /14.01.001/2011 -12 dated April 17, 2012	Know your Customer (KYC) guidelines - accounts of proprietary concerns	An addition is made to the list of documents that may be accepted for opening a bank account in the name of a sole proprietary concern
49	DBOD. AML.BC. No 109 /14.01.001/2011 -12 dated June 08, 2012	Know your Customer (KYC) guidelines- Unique Customer Identification Code for bank customers in India	Banks to introduce Unique Customer Identification system to track all facilities availed, monitor transactions in a holistic manner and to have better risk-profiling of customers. System should be in place by May 2013.
50.	DBOD. AML.BC. No 110 /14.01.001/2011 -12 dated June 08, 2012	Know your Customer (KYC) guidelines - Risk Categorization and updation of Customer Profile	Banks advised to complete the work of risk categorization and updation of risk profile of all customers by March 2013.
51	DBOD.AML.BC. No. 39/14.01.001/20 12-13 dated September 7, 2012	Uploading of Reports in 'Test Mode' on FINnet Gateway	FIU-IND has advised that all banks should initiate submission of reports on the FINnet Gateway in TEST MODE from August 31, 2012 to test their ability to upload the report electronically.
52	DBOD.AML.BC. No. 49/14.01.001/20 12-13 dated September 7, 2012	Uploading of Reports in 'Test Mode' on FINnet Gateway	FIU-IND has advised that all banks should 'go-live' from October 20, 2012 and banks may discontinue submission of reports in CD format and use only FINnet Gateway for uploading of reports in the new XML reporting format.
53	DBOD.AML.BC. No. 65/14.01.001/20 12-13 dated December 10,	Know Your Customer (KYC) norms /Anti-Money Laundering	KYC norms were further simplified by issuing following instructions : (i) to have only one document for both identity and address if the address on the document

95

Sr. No.	Circular No. and date	Subject	Gist of instructions
	2012	(AML) Standards/Combating of Financing of Terrorism (CFT)/Obligation of banks under Prevention of Money Laundering Act (PMLA), 2002	submitted for identity proof is same as that declared in the account opening form, (ii) introduction from an existing customer of the bank not mandatory when documents of identity and address are provided, (iii) If the address provided by the account holder is the same as that on Aadhaar letter, it may be accepted as a proof of both identity and address, (iv) NREGA Job Card to be accepted as an 'officially valid document' for opening of bank accounts without the limitations applicable to 'Small Accounts'
54	DBOD.AML.BC. No.71/14.01.001 /2012-13 dated January 18, 2013	Know Your Customer (KYC) Norms /Anti-Money Laundering (AML) Standards/Combating of Financing of Terrorism (CFT)/Obligation of banks under Prevention of Money Laundering Act (PMLA), 2002	Procedure to identify beneficial owner as advised by Government has been specified.
55	DBOD.AML.BC. No. 78 /14.01.001/2012 -13 dated January 29, 2013	Know Your Customer (KYC) Norms /Anti-Money Laundering (AML) Standards/Combating of Financing of Terrorism (CFT)/Obligation of banks under	To help a large number of customers with transferable jobs or those who migrate for jobs are unable to produce a utility bill or other documents in their name as address proof immediately after relocating, banks were advised to transfer existing accounts at the transferor branch to the transferee branch without insisting on fresh proof of address

96

Sr. No.	Circular No. and date	Subject	Gist of instructions
		Prevention of Money Laundering Act (PMLA), 2002	and on the basis of a self-declaration from the account holder about his/her current address, subject to submitting proof of address within a period of six months. Further, banks were also advised to accept rent agreement duly registered with State Government or similar registration authority indicating the address of the customer, in addition to other documents listed as proof of address in Annex I of our Master Circular on KYC/AML/CFT dated July 2, 2012.
56	RBI/2012-13/459 DBOD.AML.BC. No.87/14.01.001 /2012-13 dated March 28, 2013	Simplifying norms for Self Help Groups	KYC verification of all the members of SHG need not be done while opening the savings bank account of the SHG and KYC verification of all the office bearers would suffice. As regards KYC verification at the time of credit linking of SHGs, no separate KYC verification of the members or office bearers is necessary
57	DBOD. AML.BC. No.101 /14.01.001/2011 -12 dated May 31, 2013	Extending time period for allotting Unique Customer Identification Code (UCIC) for banks' customers in India	Considering the difficulties experienced in implementation the time for completing the process of allotting UCIC to existing customers was extended up to March 31, 2014.
58	DBOD.AML.BC. No.29 /14.01.001/2013 -14 dated July 12, 2013	To reiterate and strengthen certain existing guidelines on KYC/AML/CFT for strict compliance.	Investigations by the Reserve Bank in the light of alleged violation of KYC/AML guidelines by several banks have shown that these guidelines have been violated, particularly in the case of walk-in customers. The circular was issued to reiterate and

97

Sr. No.	Circular No. and date	Subject	Gist of instructions
			strengthen certain existing guidelines on KYC/AML/CFT for strict compliance.
59	DBOD.AML.BC. No. 34/14.01.001/2013-14 dated July 23, 2013	Simplifying norms for Periodical Updation of KYC	The issue was reviewed in the light of practical difficulties/constraints expressed by bankers/customers in obtaining/submitting fresh KYC documents at frequent intervals as the relative documents submitted earlier specially by low-risk customers have remained unchanged in most of the accounts. Accordingly, based on the suggestions received, revised instructions were received.
60	DBOD.AML.BC. No.44/14.01.001/2013-14 dated September 2, 2013	e-KYC Service of UIDAI – Recognising on-line Aadhaar authentication (electronic verification process) to be accepted as an 'Officially Valid Document' under PML Rules	In order to reduce the risk of identity fraud, document forgery and have paperless KYC verification, e-KYC service UIDAI has launched its. Accordingly, it has been decided to accept e-KYC service as a valid process for KYC verification under Prevention of Money Laundering (Maintenance of Records) Rules, 2005
61	DBOD.AML.BC. No.45/14.01.001/2013-14 dated September 2, 2013	Foreign students studying in India – KYC procedure for opening of bank accounts	Considering the difficulties faced by foreign students arriving in India in complying with the Know Your Customer (KYC) norms while opening a bank account due to non-availability of any proof of local address, norms were relaxed by allowing a time of one month for furnishing the proof of local address.
62	DBOD. AML.BC. No. 50/14.01.001/2013-14 dated September 3,	Circular regarding Information sought by banks from customers	Banks were advised to collect only 'mandatory' information required for KYC purpose while opening an account and Other 'optional' customer

Sr. No.	Circular No. and date	Subject	Gist of instructions
	/2013-14 dated December 31, 2013	PML Act	Boards as "designated Director" to ensure compliance with the obligations under Section 13(2) of the Prevention of Money Laundering (Amendment) Act, 2012.
65	DBOD.AML.BC. No. 100/14.01.001/2013-14 dated March 4, 2014	Recognising E-Aadhaar as an 'Officially Valid Document' under PML Rules	Banks have been advised to accept e-Aadhaar downloaded from UIDAI website as an officially valid document subject to the following: a) If the prospective customer knows only his/her Aadhaar number, the bank may print the prospective customer's e-Aadhaar letter in the bank directly from the UIDAI portal; or adopt e-KYC procedure as mentioned in the circular referred in paragraph 2 above. b) If the prospective customer carries a copy of the e-Aadhaar downloaded elsewhere, the bank may print the prospective customer's e-Aadhaar letter in the bank directly from the UIDAI portal; or adopt e-KYC procedure as mentioned in the circular referred in paragraph 2 above; or confirm identity and address of the resident through simple authentication service of UIDAI.
66	DBOD. AML. No. 16415 /14.01.001/2013 -14 dated March 28, 2014	Reporting of Cross Border Wire Transfer Report on FINnet Gateway	As per advice of FIU-IND a new reporting format for reporting of cross border wire transfers has been introduced. This was necessitated by amendments to Prevention of Money Laundering (PML) Rules, notified by the Government of India vide Notification No. 12 of 2013 dated August 27, 2013 and in terms of amended Rule 3, every reporting

100

Sr. No.	Circular No. and date	Subject	Gist of instructions
			entity is required to maintain the record of all transactions including the record of all cross border wire transfers of more than Rs. 5 lakh or its equivalent in foreign currency, where either the origin or destination of the fund is in India.
67	DBOD.AML.BC. No.103/14.01.001/2013-14 dated April 3, 2014	Harmonization of KYC norms for Foreign Portfolio Investors (FPIs)	KYC norms in case of FPIs for opening bank accounts were rationalised of along the lines of instructions issued by SEBI.
68	DBOD.AML.BC. No. 119/14.01.001/2013-14 dated June 9, 2014	Clarification on Proof of Address	Norms for furnishing proof of address have been relaxed to allow submitting only one documentary proof of address (either current or permanent) while opening a bank account or while undergoing periodic updation. It was also advised that in case the address mentioned as per 'proof of address' undergoes a change, fresh proof of address may be submitted to the branch within a period of six months. In case the proof of address furnished by the customer is not the local address or address where the customer is currently residing, the bank may take a declaration of the local address on which all correspondence will be made by the bank with the customer. No proof is required to be submitted for such address for correspondence/local address. This address may be verified by the bank through 'positive confirmation' such as acknowledgment of receipt of (i) letter, cheque books, ATM cards; (ii) telephonic conversation; (iii)

101

Sr. No.	Circular No. and date	Subject	Gist of instructions
			visits; etc. In the event of change in this address due to relocation or any other reason, customers may intimate the new address for correspondence to the bank within two weeks of such a change.
69	DBOD. AML.BC. No.124 /14.01.001/2013 -14 dated June 26, 2014	Unique Customer Identification Code (UCIC) for banks' customers in India	In view the requests received, from banks for allowing more time to complete the exercise of allotting UCIC to existing customers, it was decided to extend the time for completing the process of allotting UCIC to existing customers up to December 31, 2014.

ANNEX-IV/2

102

भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA
www.rbi.org.in

RBI/2013-14/209
DBOD.AML.BC. No. 44 /14.01.001/2013-14 September 2, 2013

The Chairmen / CEOs of all Scheduled Commercial Banks
(Excluding RRBs)/Local Area Banks / All India Financial Institutions

Dear Sir,

Know Your Customer (KYC) Norms /Anti-Money Laundering (AML) Standards/ Combating of Financing of Terrorism (CFT)/Obligation of banks under Prevention of Money Laundering Act (PMLA), 2002 – e-KYC Service of UIDAI – Recognising on-line Aadhaar authentication (electronic verification process) to be accepted as an 'Officially Valid Document' under PML Rules

Please refer to paragraph 2.6 (B) (a) of our Master Circular DBOD.AML.BC. No. 24/14.01.001/ 2013-14 dated July 1, 2013 on Know Your Customer (KYC) Norms / Anti-Money Laundering (AML) Standards/Combating of Financing of Terrorism (CFT)/Obligation of banks under PMLA, 2002 which states that letter issued by the Unique Identification Authority of India (UIDAI) containing details of name, address and Aadhaar number may be accepted as an 'Officially Valid Document'. Further in terms of paragraph 2.6 (B) (d) of the Master Circular it has been advised to banks that, while opening accounts based on Aadhaar, if the address provided by the account holder is the same as that on Aadhaar letter, it may be accepted as a proof of both identity and address.

2. In order to reduce the risk of identity fraud, document forgery and have paperless KYC verification, UIDAI has launched its e-KYC service. Accordingly, it has been decided to accept e-KYC service as a valid process for KYC verification under Prevention of Money Laundering (Maintenance of Records) Rules, 2005. Further, the information containing demographic details and photographs made available from UIDAI as a result of e-KYC process ("which is in an electronic form and accessible so as to be usable for a subsequent reference") may be treated as an 'Officially Valid Document' under PML Rules. In this connection, it is advised that while using e-KYC service of UIDAI, the individual user has to authorize the UIDAI, by explicit consent, to release her or his identity/address through biometric authentication to the bank

बैंकिंग परिचालन और विकास विभाग, केंद्रीय कार्यालय, केंद्रीय कार्यालय भवन, 13वीं मंजिल, शहीद भगत सिंह मार्ग, मुंबई – 400 001
फोन: 022-22701223, फैक्स: 022-22701239, ईमेल-: cgmicdbodco@rbi.org.in, वेबसाइट: www.rbi.org.in
Department of Banking Operations & Development, Central Office, Central Office Building, 13th Floor, Shahid Bhagat Singh Marg, Fort, Mumbai – 400 001
Phone : 022-22701223, Fax : 022-22701239, E-mail : cgmicdbodco@rbi.org.in, Website : www.rbi.org.in

हिंदी आसान है, स्वयं प्रयोग बढ़ाइए

"Caution: RBI never sends mails, SMSs or makes calls asking for personal information like bank account details, passwords, etc. It never keeps or offers funds to anyone. Please do not respond in any manner to such offers."

branches/business correspondents (BCs). The UIDAI then transfers the data of the individual comprising name, age, gender, and photograph of the individual, electronically to the bank/BCs, which may be accepted as valid process for KYC verification. The broad operational instructions to banks on Aadhaar e-KYC service is enclosed as Annex.

3. Banks are advised to have proper infrastructure (as specified in Annex) in place to enable biometric authentication for e-KYC.

4. Physical Aadhaar card/letter issued by UIDAI containing details of name, address and Aadhaar number received through post would continue to be accepted as an 'Officially Valid Document'.

5. Banks may revise their KYC policy in the light of the above instructions and ensure strict adherence to the same.

Yours faithfully,

(Prakash Chandra Sahoo)
Chief General Manager

Annex

Operational Procedure to be followed by banks for e-KYC exercise

The e-KYC service of the UIDAI is be leveraged by banks through a secured network. Any bank willing to use the UIDAI e-KYC service is required to sign an agreement with the UIDAI. The process flow to be followed is as follows:

1. Sign KYC User Agency (KUA) agreement with UIDAI to enable the bank to specifically access e-KYC service.
2. Banks to deploy hardware and software for deployment of e-KYC service across various delivery channels. These should be Standardisation Testing and Quality Certification (STQC) Institute, Department of Electronics & Information Technology, Government of India certified biometric scanners at bank branches/ micro ATMs/ BC points as per UIDAI standards. The current list of certified biometric scanners is given in the link below: http://www.stqc.gov.in/sites/upload_files/stqc/files/UID_Auth_Certlist_250613.pdf
3. Develop a software application to enable use of e-KYC across various Customer Service Points (CSP) (including bank branch, BCs etc.) as per UIDAI defined Application Programming Interface (API) protocols. For this purpose banks will have to develop their own software under the broad guidelines of UIDAI. Therefore, the software may differ from bank to bank.
4. Define a procedure for obtaining customer authorization to UIDAI for sharing e-KYC data with the bank. This authorization can be in **physical** (by way of a written explicit consent authorising UIDAI to share his/her Aadhaar data with the bank/BC for the purpose of opening bank account) /**electronic** form as defined by UIDAI from time to time.
5. Sample process flow would be as follows:
    a. Customer walks into CSP of a bank with **his/her 12-digit Aadhaar number and explicit consent** and requests to open a bank account with Aadhaar based e-KYC.
    b. Bank representative manning the CSP enters the number into bank's e-KYC application software.
    c. The customer inputs his/her biometrics via a UIDAI compliant biometric reader (e.g. fingerprints on a biometric reader).
    d. The software application captures the Aadhaar number along with biometric data, encrypts this data and sends it to UIDAI's Central Identities Data Repository (CIDR).
    e. The Aadhaar KYC service authenticates customer data. If the Aadhar number does not match with the biometrics, UIDAI server responds with an error with various reason codes depending on type of error (as defined by UIDAI).
    f. If the Aadhaar number matches with the biometrics, UIDAI responds with digitally signed and encrypted demographic information [Name, year/date of birth, Gender, Address, Phone and email (if available)] and photograph. This information is captured by bank's e-KYC application and processed as needed.

g. Bank's servers auto populate the demographic data and photograph in relevant fields. It also records the full audit trail of e-KYC viz. source of information, digital signatures, reference number, original request generation number, machine ID for device used to generate the request, date and time stamp with full trail of message routing, UIDAI encryption date and time stamp, bank's decryption date and time stamp, etc.
h. The photograph and demographics of the customer can be seen on the screen of computer at bank branches or on a hand held device of BCs for reference.
i. The customer can open bank account subject to satisfying other account opening requirements.

True Copy